Privacy Policy-Based Framework for Privacy Disambiguation in Distributed Systems

PhD Thesis

Dhafer Alhalafi

This thesis is submitted in partial fulfilment of the requirements

For the degree of Doctor of Philosophy

Software Technology Research Laboratory

De Montfort University

United Kingdom

November 2015

Dedication

Especially to my beloved Family

This thesis is dedicated to my mother who passed away from this world during my studies, she always encouraged me and hoped that I would complete my PhD and to my Father who has been my supportive, motivated, inspired guide throughout my life, and to my beloved Family, My Wife for her support and patience throughout my PhD.

To my Sisters and Brothers for their support, prayers and encouragement throughout my entire life.

Abstract

With an increase in the pervasiveness of distributed systems, now and into the future, there will be an increasing concern for the privacy of users in a world where almost everyone will be connected to the internet through numerous devices. Current ways of considering privacy in distributed system development are based on the idea of protecting personally-identifiable information such as name and national insurance number, however, with the abundance of distributed systems it is becoming easier to identify people through information that is not personally-identifiable, thus increasing privacy concerns. As a result ideas about privacy have changed and should be reconsidered towards the development of distributed systems. This requires a new way to conceptualise privacy. In spite of active effort on handling the privacy and security worries throughout the initial periods of plan of distributed systems, there has not been much work on creating a reliable and meaningful contribution towards stipulating and scheming a privacy policy framework. Beside developing and fully understanding how the earliest stage of this work is been carried out, the procedure for privacy policy development risks marginalising stakeholders, and therefore defeating the object of what such policies are designed to do. The study proposes a new Privacy Policy Framework (PPF) which is based on a combination of a new method for disambiguating the meaning of privacy from users, owners and developers of distributed systems with distributed system architecture and technical considerations. Towards development of the PPF semi-structured interviews and questionnaires were conducted to determine the current situation regards privacy policy and technical considerations, these methods were also employed to demonstrate

the application and evaluation of the PPF itself. The study contributes a new understanding and approach to the consideration of privacy in distributed systems and a practical approach to achieving user privacy and privacy disambiguation through the development of a privacy button concept.

Declaration

I declare that the main text in this thesis is all my own work undertaken by me for the degree of Doctor of Philosophy, at the software Technology Research Laboratory (STRL), at De Montfort University, United Kingdom and that it has not previously been submitted for any academic award or qualification apart from the one for which it is now being submitted.

Signed: Dhafer Alhalafi

Publications

- Alhalafi, D. (2015). A New Methodology to Disambiguate Privacy. *ACTA PHYSICA POLONICA A*. 28 (2B), 319 - 323.

- Alhalafi D. (2015). Privacy Policy-Based Framework for distributed system based on privacy disambiguation, ICCESEN 2015. Antalya.

Acknowledgement

First and foremost, I would like to express my deepest gratitude to God (Allah) for giving me the strength to carry on. I would also like to thank my supervisor Dr. Francois Siewe for guiding and encouraging me throughout my PhD. He always provided me useful comments and suggestions regarding my research. My heartfelt thanks also go to my previous supervisor Professor Hussein Zedan.

My many thanks would go to my second supervisor Professor Liming (Luke) Chen and my advisors Dr. Helge Janicke who have given me some of their precious time to comment on my work.

I would also like to thank De Montfort University for providing a studious environment and good facilities with which to complete this research. I would like to thank my family for their patience during our in the UK.

Finally, I would like to thank other STRL staff and all my colleagues for the valuable advice and discussions.

Table of Contents

Dedication ……..…….. I

Abstract……..…..…….II

Declaration ……..……..……...…….III

Publications …..……..……..…….....IV

Acknowledgement …..……...……...……...…….....V

Table of Content ……..……..…….. VI

List of Tables ……..……...…..XII

List of Figures ……..…….XIII

List of Abbreviation ……..……XIV

CHAPTER 1

1.1 Introduction…..……...…….……..……..2

1.1.2 Classical approach to privacy and confidentiality ……..…..…4

1.1.3 The Missing link between technology and Privacy policy ……..….5

1.1.4 How current privacy policies fail invasive distributed system…….....6

1.2 Problem Statement……...……..……7

1.3 Research Questions……..…..……....7

1.4 Aims and Objectives……...……..….8

1.5 Scope of the Research……..……..9

1.6 Methodology……...…….....10

1.7 Success Criteria……..……11

1.8 Thesis Outline……..……11

CHAPTER 2

Literature Review……..……13

2.1 Introduction….……..……..……..……..14

2.2 Privacy…….15

2.2.1 The Meaning of Privacy……...……...17

2.2.2 Demand for Privacy……...……..19

2.2.3 Privacy Perception……...……20

2.2.4 Privacy Disambiguation……..……22

2.2.5 Concerns about Privacy……...……24

2.2.6 Threat of Privacy and the Internet...……26

2.2.7 Anonymity……...27

2.2.7.1 Anonymisation and Data Sharing……30

2.2.7.2 The Anonymisation Trace Problem…….31

2.2.8 Distributed Systems…….32

2.2.8.1 Privacy in Distributed Systems – Limitations and Problems.....35

2.3 Privacy and Security……36

2.3.1 Privacy and Software / Hardware ….……..39

2.3.1.1 Privacy and Software……...……39

2.3.1.2 Privacy and Hardware……...……..…40

2.4 Privacy Frameworks……...…….41

2.4.1 Developing Privacy Policy Frameworks……...……..44

2.5 Structuration Theory……..…..……45

2.6 Related Work…….....…47

2.7 Summary……..……49

CHAPTER 3

Methodology……...……50

3.1 Introduction.……...……...……..51

3.2 Theoretical Foundation and Methodological Approach……...…….....54

3.2.1 Descriptive Approach……...……54

3.2.2 Quantitative Research……...……55

3.2.3 Qualitative Research……..……..56

3.2.4 Structuration Theory……..…….....57

3.2.5 Mixed Methods Approach……..…….59

3.3 Research Method……...……..60

3.3.1 Semi-Structured Interviews……..……...……61

3.3.2 Development of Interview……...……63

3.3.3 Piloting……..…….……..64

3.3.4 Sampling for Interview……..…….….64

3.3.5 Conducting the Interview……..…….….65

3.3.6 Interview Analysis…….…….……65

3.3.7 Qualitative Analysis……..…….…….66

3.4 Questionnaires……...…..66

3.4.1 Development of Questionnaire……67

3.4.2 Administrating the Questionnaire……...…….71

3.4.3 Questionnaire Sampling……..……71

3.4.4 Piloting the Questionnaire……...……72

3.4.5 Questionnaire Analysis……...…….72

3.5 Post PPF Development Questionnaire ……72

3.6 Analysis Methods……..……...……...…….73

3.6.1 Quantitative Analysis……..……73

3.7 Ethical Considerations…….74

3.8 Summary……..……75

CHAPTER 4

Privacy Policy Framework Design…….……..76

4.1 Introduction…….……77

4.2 Overview of Privacy Policy Framework (PPF)……...77

4.3 Background……..80

4.4 Privacy Disambiguation……..……82

4.5 Hybrid Privacy Terms in DS……...…....84

4.5.1 Primary Specification…….…….85

4.5.2 Secondary Specification…….…….85

4.6 Privacy Button……...……...…...87

4.7 Summary……..……90

CHAPTER 5

Application of Framework- Result Analysis……..….91

5.1 Introduction……...……...…92

5.2 Lexical……..……..92

5.2.1 Privacy Disambiguation-perceptions…..……..…93

5.2.2 From Perception- Expectation……..……..……93

5.3 Technical……..……..……95

5.4 Hybridisation of Lexical and Technical Terms……...……....96

5.5 Practical Application of PPF……..……97

5.6 Current Privacy Policy and Privacy in DS……...……...97

5.6.1 Results of Experts Interviews……..……..…….97

5.6.2 Results of Questionnaires – users and developers…….……100

5.7 Privacy Perception…….……115

5.8 Lexical Technical Terms for Privacy Policy…….122

5.9 Summary……..……..124

CHAPTER 6

Discussion and Evaluation ……...……..…126

6.1 Introduction……...……127

6.2 Findings Interviews……...……129

6.3 Findings Questionnaire……..131

6.4 Implications of Findings- Is Privacy perception Measurable.....135

6.5 Summary……..……...……..136

CHAPTER 7

Conclusion and Future Work……...……..137

7.1 Conclusion……...……..138

7.2 Contributions……...……..140

7.3 Success Criteria…….142

7.4 Limitations…….143

7.5 Future Study……..……144

Bibliography……...……..147

Appendix……...…….……...……158

Interview Schedule…….....158

Questionnaire……...……...……..158

List of Tables

Table 3.1 Qualitative and Quantitative Methods……..…..…59

Table 4.1 Framework Factors hybrid privacy system……...…….86

Table 5.1 Derived perceptions to expectations……..……94

Table 5.2 Opinions about the enterprise privacy policy……..…..103

Table 5.3 Event for privacy policy protection……..……105

Table 5.4 Concern for potential privacy Violation……....107

Table 5.5 Effectiveness of Privacy policy……...…..108

Table 5.6 Agreement with Privacy policy ideas……....109

Table 5.7 Agreement with user's consultation for privacy policy.....111

Table 5.8 Consultation method for personal privacy needs……..113

Table 5.9 Awareness for Information disclosure…….…….116

Table 5.10 Need for personal information disclosure……..……..117

Table 5.11 Ability to control private Information disclosure ……...….118

Table 5.12 Mechanism for full control private Information disclosure.119

Table 5.13 Preference for logging of personal information……..…….120

Table 5.14 Preference on ability to adjust involvement in privacy…...121

Table 5.15 Lexical – Technical Terms for Privacy Policy…….……123

List of Figures

Figure 2.1 Anonymising process using Encrypting…….…….30

Figure 3.1 Methodology Framework……...…..……53

Figure 4.1 Privacy Policy Framework (PPF)…….……..……..…79

Figure 4.2 Illustration user Privacy input captured……..…..89

Figure 4.3 HPTM method application illustrations…….……..…89

Figure 5.1 Awareness of the function of privacy users and developers.101

Figure 5.2 Area for concern for potential privacy violations……107

Figure 5.3 A graph for agreement with idea on privacy policy…...….110

Figure 5.4 A graph showing consultation of privacy policy……..…112

Figure 5.5 A graph showing methods of consultation……..…….113

Figure 5.6 References to logging personal information……..……120

Lest of Abbreviation

PPF	Privacy Policy Framework
DS	Distributed Systems
U2U	User 2 User
HPTM	Hybrid-Privacy Terms Methodology
ICT	Information Communication Technology
GPS	Global Positioning System
HIPAA	Health Insurance Portability and Accountability Act
CPU	Central Processing Unit
I/O	Input / Output
RFID	Radio Frequency Identification
AI	Artificial Intelligence

Chapter 1

Introduction

Objectives

- Provide an introduction along with the motivation for this research.
- Highlight the research questions and the success criteria.
- Outline the main contribution of this research.
- Present the research methodology and thesis structure.

1.1 Introduction

This study presents a framework for the disambiguation of privacy for the development of privacy policies in distributed systems. It is based on the idea that privacy is something that is not sufficiently considered in the development of such privacy policies, especially in terms of what privacy means to people subjectively. The disambiguation of privacy in this study involves understanding descriptions of privacy from the perspective of users of distributed systems as such perceptions will change with the ever changing developments in technology. Moreover, the disambiguation of privacy also involves understanding the technical implications of privacy, for example what should the technology provide in terms of providing for privacy and its limitations in this regard. The Cambridge dictionary defines privacy as "*someone's right to keep their personal matters and relationships secret"* (Cambridge Dictionaries Online, 2014). Here there is a clear reference to the right to privacy. Moreover, in their example beneath this definition the Cambridge dictionary clearly emphasises that privacy is something that needs protecting: *The new law is designed to protect people's privacy.* The Merriam Webster dictionary defines privacy as: "*The quality or state of being apart from company or observation* and *Freedom from unauthorised intrusion"* (Merriam Webster, 2014). The latter definition refers to a person's right to privacy protection.

In a world where computers govern many aspects of our daily lives, privacy or information privacy is the protection of data that contains our personal information from being accessed by unauthorised individuals, and includes issues such as data collection, dissemination, privacy expectation, political issues, legal issues and technology issues

(Carroll, 2006. There are several types of personal information that require privacy and include educational, medical, political, internet, locational and financial (Stahl, 2004).

Privacy is becoming fundamental for individuals, organisations and governments. Privacy is the top priority of governments around the world, in particular western nations (Lee, 2013). It is important to note that information and communication technology (ICT) has caused doubling effects on human knowledge and enabled its fast accumulation, especially in the sciences and technology while globalisation appears to shrink geographical distances and time; and all types of information flows through communication networks, both wired and wireless, mean that all of humanity is plugged into an interconnected network, that provides for interactions and transactions (Schneier, 2013).

All connected to the next-generation internet using abundant, low-cost, and high-power computing (Winter, 2012)

In order to expatiate on the revolutionary Internet of Things, there is a need to bring up to notice the privacy surveillance so that important factors can be traced, monitored, located and measured via advanced technologies such as sensor networks, radio frequency, energy harvesters, as well as embedded services. These serves as sources accessories to the next internet generation technology by using very resourceful low cost and more advance computing (Winter, 2012).

Monitoring public and private networks has become the prime tool in fighting and preventing crime. Monitoring devices are far from understanding and acting on human notions of privacy and liberty. This research will disambiguate the meaning of privacy

for developers and users and the concepts, principles and methods of technology in relation to privacy. The aim is to bridge the gap existing between technology developers and individuals within the context of privacy. However, the data flow out of individuals and organisations may lead to unpredictable and unexpected results and consequences. There are organisations that have reason to believe harvesting these data can improve and maximise efficiency and therefore revenue. Therefore, there is a need to ensure that the privacy needs of users are considered when developing privacy policies, unfortunately, this is not always achieved.

1.1.2 Classical approach to privacy and confidentiality

Conventionally, privacy policy has concentrated on a controlled data, that are more related to personal identity for instance, phone numbers, names and date of birth or national Insurance number which is virtually linked to individual personal data. The personal identifiable information strategy is used by organisations as well as for other important purposes. However, this information must be protected by law to safeguard the privacy of the owner. Moreover, other information which is not classified under this category includes personal sensitive data such as religious beliefs, political affiliation and health status (Data Protection Act 1998 s.2).

To demonstrate this situation is the typical example of where you live, the data your share through your post code, combination of your date of birth? There are almost none. Though, studies revealed that about 97% within the population of Americans the three unique combination of information form a basic identity (Cranor et al, 2000).

1.1.3 The missing link between technology and privacy policy

Privacy policies often fail in terms of the way that they communicate data handling practices and they are often not transparent, the lexicology that is used in privacy policy should be more exact in order to increase transparency and improve user trust in using the internet (Pollach, 2008).

In addition to security concerns about information systems, consumers are increasingly concerned about the use, treatment and even transfer of their private data, in fact 40 percent of people feel that their private data is in jeopardy and 45 percent feel that laws are not enough to protect them (Flavian and Guinaliu, 2006). Anton et al. (2010) identify six areas of privacy concern for users of the internet which include awareness, information collection, storage and transfer and access, moreover, there has been an evolution in these concerns due to the increase in social media websites where users can connect with a variety of people including colleagues, friends and families.

Other areas of concern for users of the internet are the type of information that a web site will collect from them, the level of control that the users have over that information and the awareness of the privacy policies, however, it is also important to note that there are factors such as intrinsic beliefs, perceptions, web site related variables and situation variables that have an effect on privacy perception (Mekovec and Vrcek, 2011).

1.1.4 How current privacy policies fail invasive distributed System

Just as life goes on with daily routine, our identity are risked as our information are fetched without our consent in an indefinite manner either by customer services advisors while we pay our bills or through our debit and credit cards when we shop online. This companies stores our data and shared it to other companies for marketing purposes without our knowledge (Gong et al, 2014). When we pay in cheque, lodge monies, use or royalties or discount cards, the supermarkets and allied build in a database with the information (Sandhu et al, 2011). These same information tactics is also used by the insurance and motorist companies which detect our locations and out base at any time including our debit cards details. (Xie et al, 2006). When we surf the internet, brows or carry an online shopping, we leave a very significant trail of our data. This is also possible when we subscribe to and online, regular magazine, newsletters, club membership, professional bodies or guarantee cards to donate monies to charities.

This is also the case when we invest money, when we make a telephone call, when we interact with a government agency, then we leave our data trail automatically saved in our computers Gasser et al, 2009).

Tracking location is not a new revolution, it is the combination of many techniques and tricks of Morden technology which is run by many ways including wireless or cellular devices that gives signal to a certain radios (Winter, 2012) The following are basically the three common techniques used even though, some more sophisticated technology is researching and building more sensible tracking devices technologies:

- Satellite radios signals rays can be traced and compared via the GPS technology.
- Triangulation sources signals directional from cell phone antennas.
- Wi-Fi and local area networks trace high-frequency radio signals from Transmitters.

1.2 Problem Statement

Systems are becoming increasingly complex and distributed which is creating new considerations for user privacy. All too often privacy policy that is written for distributed systems is established as a purely technical policy and does not consider the privacy needs of the user. Even where such needs are considered they do not consider the perception of users and what they feel privacy really is. Therefore, there is a need to understand users' perception of privacy through which user expectations can be derived.

1.3 Research questions:

1. How can distributed system architecture be combined with a structuration theory approach for privacy disambiguation?

2. Can a better understanding of privacy through privacy disambiguation lead to an improved privacy policy for distributed systems?

3. Can privacy within an organisation be achieved via a Privacy Policy-Based Framework?

Derived from the main research questions are **sub questions** which relate to the subjective and objective elements of the structuration theory approach.

What are the subjective perceptions of privacy among developers, owners and users of distributed systems? (Question 2)

What are the factors behind effective privacy policy within an organisation? (Question 3)

What are the barriers to achieving privacy within an organisation? (Question 3)

1.4 Aims and Objectives

The aim of this research is to design and develop a Privacy Policy-Based Framework for distributed system based on privacy disambiguation.

To meet the above aim, the following objectives will be achieved:

1. To disambiguate the meaning of privacy for developers, owners and users of distributed systems.
2. To investigate how privacy and privacy policy operate within an organisational context.

3. To understand privacy in the context of system architecture and functional requirements.

4. To show how services that require access to data can be conducted without privacy.

5. To develop a Privacy Policy-based framework based on privacy disambiguation of stakeholders and system architecture.

1.5 Scope of the Research

Firstly, the scope of the study extends to the stakeholders of distributed systems, including users, owners and developers and their semantic concept (perception) of privacy towards disambiguating its meaning. Secondly, the study extends to the pragmatic concept (or understanding) of privacy in relation to the pragmatic considerations of distributed systems including their architecture and functions.

The scope of the study is on the development of a Privacy Policy Framework (PPF) that is supported by a set of recommendations for distributed system users. Both the PPF framework and the set of recommendations are aimed at translating privacy issues and needs in to a successful implementation of privacy within the organisation. This is to overcome the obstacles that have resulted in unsuccessful privacy policy implementation.

The overarching intend of the research is to examine the current situation of the privacy policies implementations in an organisation, which does include planning approach, strategic objectives and priorities. One way to achieve these is by developing a

methodology in the form of expert survey, questionnaires survey. These surveys include owners, users and developers in the organisation.

1.6 Methodology

In the proposed framework there are three elements that are part of the disambiguation of privacy; they include current privacy policy (objective), opinions of current privacy policy (subjective) and privacy perception (subjective). These three elements are under the umbrella of privacy disambiguation which forms one side of the framework i.e. the lexical component. The other side of the framework is referred to as the 'technical' and includes technical considerations of privacy in distributed systems. Therefore, the methodology is designed to derive these elements from users, developers and experts of distributed systems towards the development of the proposed framework. This is achieved through interviews with experts and questionnaires with users and developers.

Both qualitative and quantitative methods will be used as a new customised methodology to meet the research objectives. A questionnaire was used to disambiguate the meaning (semantics) of privacy from the user, management (owner) and the developer within each organisation. A semi-structured interview was conducted with professional management (or experts) to determine the current state of affairs in terms of privacy policy, how they manage privacy, the pragmatic considerations. The area of the research is two organisations in the private sector in Saudi Arabia, namely; Al Rajhi Bank, Northern Cement Company and one in the government sector; the Technical and Vocational Training Corporation. Although the research area is in Saudi Arabia, it is important to

note that the study is general and is applicable to a global context, where Saudi Arabia is merely the case study. More details on the research methodology are given in chapter 3.

1.7 Success Criteria

The following are the success criteria for the study:

- Successful disambiguation of the meaning of privacy to users.
- Translation of user perception of privacy into user expectations.
- Development of PPF based on ideas found in structuration theory and hybridisation.

1.8 Thesis Outline

Chapter 2 reviews related work related to privacy and its meaning both literally and semantically, there is an emphasis what privacy really means to people and its disambiguation. Furthermore, there is a review of material related to privacy and software and hardware issues as well as distributed systems and privacy issues in distributed systems. Finally, there is an overview of frameworks and the development of privacy policy frameworks.

Chapter 3 presents the methodological approach and the research methods that are employed. Specifically, this includes the theoretical foundations for the methodology and

the use of questionnaires and interviews. There is particular attention to paid to how the research instruments contribute to the aims and objectives of the study. Moreover, how the research is conducted, the sampling and the ethical issues are also addressed.

Chapter 4 describes the need for a privacy based policy framework. It proposes a privacy-based framework and describes how the framework is based on the idea of a hybridisation of the technical considerations for privacy in distributed systems and the privacy expectations of users based on the disambiguation of privacy.

Chapter 5 presents the results of the questionnaires and interviews. Specifically, the interviews were conducted with experts and the associated results relate to the existing situation with privacy policies in their respective organisations, and the results of the questionnaire provide information about both the existing privacy frameworks, in terms of concerns, and the perceptions of privacy among users and developers.

Chapter 6 is the discussion chapter. The results of the study and the developed privacy framework are discussed in reference to the aims and objectives of the study and the related literature. Moreover, there is a discussion of the implications of the results and the need for a new privacy policy framework.

Chapter 7 is a conclusion for the entire study, the chapter includes an overview of the findings, implications, limitations of the study and recommendations for future study.

Chapter 2

Literature review

Objectives

- To review work related to privacy and its meaning both literally and semantically.
- To review what privacy really means to people towards its disambiguation.
- To review material related to privacy and software and hardware issues.
- To review distributed systems and associated privacy issues..

2.1 Introduction

This study seeks to demonstrate the misalignment between the nature of the standard privacy policies and the privacy perceptions of the users of the distributed systems, as well as bring the highlight the need to develop the privacy policy development frameworks from the motivations of the privacy perceptions of the users. The ever-rising numbers of the privacy concerns in the use of the distributed systems are clear indications that the standardised privacy policies do not provide all the needed measures to ensure the privacy of the users of the distributed systems (Procter and Vu, 2008). However, much research (Anton et al., 2011) has been geared towards the development of the distributed systems and the development of the standardised privacy policy frameworks but there have only been a limited number of studies, such as Paine et al. (2007) and Calo (2011) that have combined the technical aspects of the privacy policy frameworks, and the distributed systems theories, with the privacy perceptions of the users to improve the privacy levels of the users, however, these studies are weak in considering the technical aspects of privacy equally with privacy perception, with more focus on the latter, in fact Rubel and Biava (2014) even go as far as completely disregard any technical aspects of privacy. As a consequence, there have been considerably major improvements in the technical components of the distributed systems without a similar improvement of the policies to meet any emerging privacy needs of the users (Procter and Vu, 2008). The present study addresses this imbalance through privacy disambiguation that considers both the technical and perception aspects of privacy equally. However, where those privacy needs have met the consideration of the perceptions of the users are limited, and the expectations of the users are not well understood. Additionally, the traditionally

developed distribution systems' Privacy Policy-Based Framework do not consider privacy disambiguation as an elementary part of the ultimate accomplishment of the users' privacy needs.

The existing literature related to this research provides the understanding of this research. The use of the existing literature in this research is limited to research papers, scholarly books, government publications, publications of authoritative organisations, and authoritative articles in the field of computing and networking related to privacy and distributed systems (Nadas, et al., 2014). In the review, the concept and the meaning of privacy are demonstrated. However, the other aspects of privacy that get redress in this review include privacy policy framework, privacy perception, security distributed systems, anonymity and structuration theory, in relation to this study.

2.2 Privacy

In the computers economy, privacy or information privacy is related to the data protection from the access of the unauthorised individuals, and it is a matrix of many variables such as data collection, dissemination, privacy expectation, political issues, legal issues and the technology (Carroll, 2006). Both the organisational and the personal information require protection from leaking to the unauthorised parties. The personal information's requirement of privacy depends on its type. There are several types of personal information that require the adherence to privacy (Stahl, 2004). These classes of information include educational, medical, political, internet, locational, financial and cable television (Data Collection Policy Prompts Privacy Concerns, 2015). Legally,

privacy is considered as part of the bill of human rights that is universal. However, the provisions of the right to privacy vary depending on the global jurisdictions and organisations always try to remain compliant to avoid the legal implications of the provision.

With the increasing use of the online social networking, more privacy concerns have emerged. The privacy issues of the social networking emerge during the attempt of the users to establish and maintain online relationships with other users and they can arise from the actions of the friends of the users or other sources not related to the relationships of the users (Anthonysamy et al., 2013). Although the social networking service providers have periodically updated privacy policies, the privacy concerns related to social networking are always evolving. The emergence of the social media has led to the development of various networks for the users, each of which has specific privacy concerns (Reenleaf et al., 2015). These networks, as indicated by Myspace, Facebook, and Friendster, include; personal networks, location networks, status update networks and content-sharing networks. These networks can expose a myriad of informational pieces such location, contacts, gender, marital status and education, amongst others (Mooradian, 2014).

On the internet, the target information privacy perspectives include such examples as age, physical address and financial information, amongst others (Park and Kim, 2014). The access to the internet by individuals is facilitated by the provision of such services as a mobile phone carrier, wireless hotspots and internet service providers (Tavani, 2007). The internet privacy concerns are related to one's presence in the online purchases, social networking applications, online forums and online games, amongst others. In these uses,

the privacy of the internet user can be compromised through the cracked passwords (Coll, 2014).

Normally, privacy is observed as a surveillance countermeasure that is allowed under the fundamental freedoms. However, with the strong emergence of the information economy it also serves as a surveillance partner-in-crime. In that view, privacy has been used as a major driver of information capitalism and thus making it a prerequisite for the blossoming of the information economy. Today, information privacy is a democratised subject to favour information capitalism. Although the concept of privacy has advanced to the power-knowledge status, there is limited understanding of the privacy conceptions between informational capitalism promoters and the promoters of freedom and democracy via privacy (Coll, 2014).

2.2.1 The Meaning of Privacy

The privacy standards aim at maintaining one's freedom from the public attention. From the legal viewpoints, privacy entails the aspect that restricts the distribution of personal information to the public by the unauthorised person. However, in today's digital economy the amount of information gathered every moment by the electronic technologies is just beyond most logical metrics. As a result, this digital age understands more about the significance of privacy both in the personal and the enterprise' life. In this age, there is a large intersection of the legal perspectives of privacy and technological uses because of the large deal of information that is irreversibly getting stored in the computer storages (Papanikolaou, et al., 2012). The personal databases created by the

digital machines create digital dossiers that present legal ties and different privacy concerns. The digital dossiers in the form of digital databases present myriad privacy threats that could cause irreparable damages to privacy (Acquisti et al., 2015). Initially, the term privacy existed without the consideration of the virtual threats and it related to physical access to personal information by unauthorised parties. However, the increase in the use of the digital tools has redefined privacy as a more sophisticated subject that relates to the virtual individuals of digital features. As a result, the legal meanings of privacy need evolution to align it with the volatile digital developments (Solove, 2004).

The business provides an avenue for product provision, innovation and job creation. Such aspects of the business can successfully be accomplished through the internet because of the wide access to the virtual marketplace. However, such aspects can only be achieved if the privacy perspectives related to the internet business are defined (Shuler, 2004). In that view, privacy exists as a measure of great online service. The privacy aspect of the UK online population is governed by the e-Privacy Directive, which guides the businesses in obtaining users' consent before using their personal information. According to the e-Privacy Directive, privacy is the aspect that allows the businesses to use the gathered information in non-intrusive, secure and transparent ways (Sevignani, 2013). It is the factor that brings the balance between the business interests and the protection of the consumers' information (Donovan, 2004).

Privacy evolves with time as a result of the developments in the technology as well as changes in the societal needs. In that view, privacy needs can never be perfectly met because of the changing nature of technologies and the human social perspectives (Hier and Walby, 2014). The motivations of the technological use and the social needs should

serve the role of benchmarking the minimum requirements of the privacy. However, the ascription value to privacy relates to the level of conflict as well as the reconciliation between privacy and other values like security, transparency, free speech and curiosity which are core to the human value systems (Doris, 2010).

For globalised business entities, the privacy responsibilities are sophisticated because of the need to protect the security of the customers', employees', and partners' personal information. In such businesses, privacy comprises the aspect of employing uniform practices of collection, use, storage, disclosure, access, processing and transfer of information only under the specific, appropriate situations (Pollach, 2007). As a result, privacy can be achieved through the application of various principles of data use and privacy such as lawful collection and processing of personal information, purposeful personal information collection, accurate and complete personal information, and appropriate personal information disclosure.

2.2.2 Demands for privacy

Industries, organisations, and governments are responsible for satisfying the demands associated with the electronic release of information as well as individual privacy whereby personal data may be disclosed. For example, for an individual who is the only male born in 1920 living in a sparsely populated area, their age, gender and zip code could be combined with voter registry information from the same area in order to obtain their name, thus revealing their medical records (Barnard, 2013).

2.2.3 Privacy Perception

Raghunathan and Chau (2006); Malik (2011), introduced different type of frameworks to help understand privacy in its entirety. For example, data type categories are considered to be high-level groupings of data, for example contact information or medical records. Such categories are employed in order to distinguish between sets of data that are required to be treated differently from point of view of privacy. Hierarchical organisation of the data improves the expressiveness of rules (Anton, et al., 2007). Once the business understands the types of personal information it must protect and knows the business purpose for using the data, the business should develop privacy policies that document the rules for collecting and sharing the information where the policies do not already exist. Others for example, Winter (2012) thought of privacy building blocks to be purely technical components. On the other hand, perceived his strategy as an amalgamation of different views of privacy, abstraction layers, and progress of customer service. He argued that these perspectives provide better understanding and visualization of privacy (Hans, 2012). Grant and Chau (2006) developed their privacy strategy to help assess, categorise and classify privacy efforts. They started from few workable definitions of privacy to figure out the building blocks (Dawes, 2008).

Primarily, the systems users link computers to various privacy issues. It is the reason for the characteristic initial reluctance in the adoption of any Internet technology that involves information sharing across the global map. In online shopping technologies, the consumers treat their engagement with contempt because of the ever-growing incidence of spoofing, spamming and cases of fraud (Al-jamal and Abu-Shanab, 2015). However, as one grows in their experience in online the perceptions of fraud threats diminishes as

they become regular online shoppers. However, the positive perceptions about online privacy or security risks increase only when the customer has consistently gotten positive experiences of online purchasing (Miyazaki & Fernandez, 2001).

With regard to the adolescent Internet users, their privacy concerns and perceptions relate to their negative interpretation of the parental control and solicitation. The boundaries of privacy made between the adolescents and their parents influence their expectations about information disclosure. As their adolescents' ages advance, the general perception of less control of their information by their parent's increases (Halboob, 2015). However, more control in late adolescence triggers the information holders' perception of privacy invasion (Hawk et al., 2008).

The websites' terms of privacy also have impacts on the private perception. Generally, a website with the terms of privacy creates a positive influence on the user perceptions of privacy. Nonetheless, the content of the terms of the website's privacy policy does not always lead to the improvement of the nature of the perceptions in terms of the trust and control (Gao and Sullivan-Gavin, 2015). The opt-in terms of the website privacy policy make the users increase the levels of control perceptions. On the other hand, the opt-in terms create decreased perceptions of control. Consequently, the website privacy policy terms create perceptions about the engagements of the user with such platforms (Manon, Jacques, Mathieu, & Anne, 2007).

The number of negative perceptions about privacy is higher in online experiences than the local organisational networks. In fact, the number of privacy issues related to the internet use is higher than it is thought. Internet users' display concern about privacy

infringement issues that are likely to lead to a leak of various forms of personal information to the public. However, most of the concerns relate to the users lack of knowledge of the functionalities of the internet (Paine et al., 2007).

2.2.4 Privacy Disambiguation

With the consideration of the stakeholders of values of privacy, it is not easy to clearly describe privacy. The complexity of the description of privacy emerges from the differences in the ideas attached to the meaning of privacy by different circles. In that view, although the technical meaning of privacy in computing and medicine, for example, may be similar, the expectations of the clients of these fields may significantly differ because of the varying expectations associated with such fields. Nevertheless, the legal idea of privacy revolves around the protection from dissemination of vital information that belongs to a specific party. The meaning of privacy varies depending on time, polity, space and the examining factors of the concept. However, the meaning does not find its basis on rigid vocabulary and thus there is a wide room for the comparisons and descriptions of the concept. In the privacy disambiguation endeavours, the description of privacy needs to consider the conceptual work as well as the philosophical ideas behind the value of privacy. Nonetheless, the true meaning of privacy is accomplishable through real situations (Rubel & Biava, 2014).

In the information age, the attainability of personal privacy goals is almost impossible because of the internet usage. Privacy has been a subject of infringement more by the internet based companies than one's closest relatives, especially for the consistent internet

users. This aspect shifts the earlier description of privacy issues as concerns produced by the personal neighbours to the concerns generated by the interactions with the internet uses. Since the evolution of the internet, distributed systems and cloud computing increases the capabilities of storing the users' internet records, the meaning of privacy also needs to evolve to include the situations under which the anonymously collected information of the users is shared (Ren, et al. 2011). More so, the use of the internet for the companies to gather personal information gives them access to intimately private information of the user, a highly penetrative aspect of privacy violation that most systems are yet to describe (Mont and Thyne, 2008). As a resultant variable, there is a rising need for research to describe digital privacy as well as track the methods that the companies use to invade personal privacy to ensure full uncovering of the concept and the unambiguous meaning of privacy (Schneier, 2013).

Privacy also includes the perceptions of the users towards the information sharing technologies. People perceive privacy as the ability to conceal ultimately their details from any person who may access it on purpose or by accident. As indicated by the RFID use and the user's privacy fears, one's privacy is significantly important that the users can prefer losing the benefits of the RFID technologies than have uncertain privacy future irrespective of the nature of the power of the privacy enhancing technologies under the use. In this view, privacy perceptions are a significant aspect of the full description of privacy (Spiekermann, 2009).

Privacy has a strongly conflicting relationship with security. In the digital age, cyber security is a prerequisite for technological applications. However, the security measures geared towards the cyber security encourage surveillance and surveillance works against

personal privacy. The surveillance practices by governments and organisations are supported by the moral, civil and legal need to offer protection to the citizenry (Kavakli, et al. 2006). For the convergence of the values of the protection of the citizenry and those of personal privacy, more details about the meaning of privacy are needed in respect to who has the authority of surveillance as well as the use of the information obtained via surveillance. In such circumstances that are related to surveillance and privacy, the meaning of privacy is squarely derived from the ethical background of the two values and practices (Van Lieshout, Friedewald, Wright & Gutwirth, 2013).

2.2.5 Concerns about Privacy

Through information technology, it has become significantly easier for personal information collection, storage, and dissemination. However, it has become more possible to use that information for social purposes such as politics and business. However, the legislations about personal information limits the use of such information because of numerous privacy-related issues and concerns that follow the inappropriate use of personal information. Privacy concerns relate to the inappropriate sharing of personal information that present threats of harms to the owner of the information. Agranoff explored the privacy concerns in relation to the legal environment. He also explored the privacy codes likely to help meet the privacy needs of an organisation. The privacy concerns are classifiable into subjective and the objective ones. The subjective concerns include the perceptions of privacy that cause alarm to the systems users. The subjective privacy concerns emerge from the fear-generating belief of being monitored (Crawford and Schultz, 2014). On the other hand, the objective privacy concerns include the unprecedented use of information against the owner. The objective concerns emanate

from the awareness that the personal information could be referred to when the second party acts against the owner. In the context of an enterprise, the information could be used to perpetrate non-conventional actions against the employees. The subjective concerns arise from the observed use of information by the companies or the unauthorised parties to perform various actions against the information owners. Calo (2011) classifies the privacy harms to help distinctively identify various aspects of privacy violations. Calo's article is highly descriptive and helps increase the knowledge of privacy. However, it is based on qualitative analysis, and thus it has various shortcomings related to qualitative research (Calo, 2011).

The privacy concerns can also be termed as malicious adversaries the limit one's privacy. In distributed systems, malicious adversaries are classifiable into the weakly and the strongly malicious adversaries. The entities that have the intentions of compromising the other's privacy are referable as weakly malicious. On the other hand, the entities that have the capabilities of using different means to cause privacy compromises are referable as strongly malicious (Shackkelford, 2004). In the distributed systems, information sharing is protectable from the malicious adversaries if all the protection goals aim at making all adversaries as weakly malicious. However, the protection is also achievable through the allowance of the trade-off between accuracy and privacy in relation to the strongly malicious adversaries. Nan and Wei (2008) description of the privacy concerns, with they describe as adversaries, is based on idealism. No numerical variables are applied in the classification of the concerns as either weakly or strongly malicious adversaries (Nan & Wei, 2008).

2.2.6 Threat to Privacy and the Internet

Use of the internet requires the involvement of a computer or a communication device. According to the Organisation for Economic Co-operation and Development it is predicted that by the year 2022, the average household will have approximately 50 devices connected to the internet. Most of these devices will broadcast to the internet automatically any human intervention. Moreover, according to Raghunathan (2013) in the future it is highly possible that almost every device could be connected to the internet.

Computer security is a field that lives in co-dependence with an adversary. The motivation for privacy and confidentiality research is ever to prevent the goals of some hypothetical wrongdoer determined to violate one of the system security policies. In general, the conceptual and motivations behind the offender are measured solely in terms of their capabilities. This approach is considered appropriate because the threat model for security mechanisms is mostly based on the offender's abilities (Loenzen-Huber, et al, 2011). Moreover, it would be erroneous to try and reason about person's state of mind as well as their behaviour. Despite this, the nature of internet-based threats has changed over recent years in such a way that we are compelled to try and develop a better understanding of modern adversaries and the mechanisms they use. Importantly, these changes include the observation that internet-based criminal activity has transformed from a reputation economy which includes defacing web sites or writing viruses, to a cash economy which includes phishing, DDoS, SPAM and extortion.

Even legal activities including vulnerability research has been motivated by the sheer power of the cash economy, and there are new vulnerabilities that are often bought and

sold by public companies and underground organisations (Garfinkel, 2008). Therefore, a large part of internet-based crime is now motivated by profit. More importantly, the nature of this activity has evolved and expanded to such an extent that it now exceeds the capacity of a closed group. As evidence of this problem, there is an active on-line market economy where trade in illicit digital goods and services takes place. Thus, while it may be difficult to analyse any villainous individual, analysing the overall market behaviour is much easier (Bynum, 2003).

2.2.7 Anonymity

The frameworks of anonymity have a wide range of capabilities of upholding privacy. In computing, the range of anonymity is related to the hierarchical level employed in the order to obtain the target level of anonymity. Depending on the hierarchical under application, there are limits because of the possible use of the identifiers to locate and identify the data, owners. In most practices, anonymity is sought through the omission of the names of the information providers but disclosing their geographical locations, their genders and sometimes the contacts. There are many anonymisation techniques available for use by the organisations to ensure the use of anonymity to promote privacy and data protection. The organisations follow specific steps to implement the anonymisation programs, which the program sponsor and the practitioner must agree. According to Raghunathan (2013), the enterprise level anonymisation has several challenges that are only addressable through the program planning. The planning phase of data

anonymisation programs address the program challenges through the identification of the techniques and patterns that are favourable to the organisation (Raghunathan, 2013).

Effective anonymisation holds potentials of benefit to the modern data uses through such aspects as medical research using hospital records. However, the concern of privacy, as well as the accuracy of the information, remains a major impediment in such uses of private information because the quasi-identifiers can effectively locate and identify the information provider. If the information recipient uses the quasi-identifiers to identify effectively the information holder, it will constitute a serious privacy breach. However, the efficient anonymisation is possible through the use of the basic frameworks of suppression and generalisation to achieve k-anonymity. For such sensitive pieces of information like those related to health, the k-anonymity can be achieved through the algorithms that have considerations for the quasi-identifiers as well as the other sensitive identification attributes (Ghinita, Karras, Kalnis & Mamoulis, 2009).
In business enterprises, especially the internet, anonymity is important because allows one to perform numerous activities without the risk of having their private information on the leak. In the payment transactions, it is possible to control anonymity to avoid ill uses. The anonymous payment systems provide ways to trace and route the anonymous parties depending on the type of the anonymity, providing means of controlling the inappropriate uses of the anonymous payment systems (Grabber, et al., 2002). The anonymous systems of transactions have numerous benefits to the personal privacy. However, the users of the anonymous systems can benefit from anonymous participation in whistleblowing, rights advocacy, counselling sessions and commercial transactions

without the disclosure of their identities. However, the anonymous transaction systems promote such harms as child pornography, financial fraud, spamming and hate emails.

The case studies point out the difficulties of data anonymisation. One example is America Online (AOL), which posted 20 million search queries online (Gong et al, 2014). The data were anonymised by removing personally-identifiable information. Regardless of removing identifiable information from the data, researchers were able to recognize precise individuals' searches. Another example was when Netflix anonymised the records of its customers, removing personally-identifiable information and assigning a sole identifier to protect and preserve continuity of its operation. A group of researchers found that by adding movie recommendations found on the internet movie database with the Netflix data, individuals could be re-identified. This example shows that, while data may appear anonymous, they can be identified when compared with other active data to increase the probability for re-identification.

One aspect of this research is that the concept of data anonymisation may appear as straightforward (Raghunathan, 2013). The principles behind introducing the anonymisation method are somehow not clear. Although the objectives behind the anonymisation method are straightforward, being namely to protect people's privacy online. Successful anonymisation will produce data that analysts will find useful, while at the same time making it impossible to identify specific individuals. However, data anonymisation might become a very complex task with a high risk of millions of pieces of personal information falling into the wrong hands. One of the best methods currently in use to provide for privacy are encryption – decryption during peer-to-peer and client-server communication (see figure 2.1). Again, re-identification or reversing the

anonymisation process of personal data can be unpredictably simple (Gong et al, 2014). For example, the method used to develop encryption algorithms may be published and widely available for public use. One more aspect is that by comparing anonymised data to other data sources, it may be possible to re-identify individuals hidden in supposedly anonymised data. These flaws can weaken the reliance that organisations place in the anonymisation process and method as a tool to protect privacy (Raghunathan, 2013).

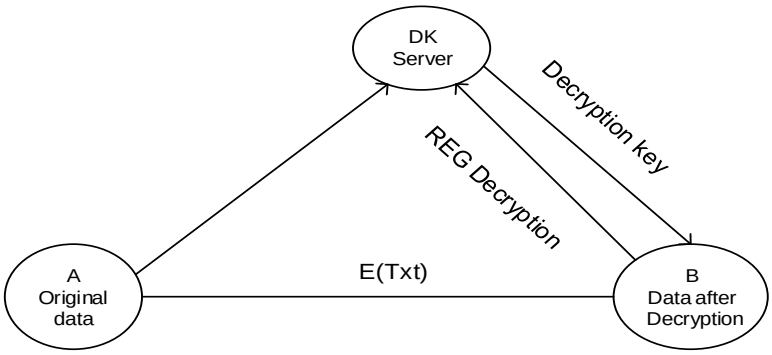


Figure 2.1: Anonymizing process using, Encrypting – Decrypting of Information method

2.2.7.1 Anonymisation and Data Sharing:

Data sharing needs balancing much privacy, security, and legal concerns (Bynum, 2003). Anonymisation of data is able to mitigate privacy concerns and be compliant with legal requirements. While anonymisation is not invulnerable, countermeasures that compromise anonymisation techniques may cause protected information to be exposed in released datasets. Moreover, those researching networking and security are engaged in research that challenges existing ethical frameworks (Kenneally, 2010). If a moral high ground is continued be occupied where the benefits of work is claimed as necessary and

the risks minimal, there is a need for more explicit justification of this reasoning to other researchers. In this chapter, we examine privacy rules, access control and XML standards. The standards seek to define a set of imperatives for distributed systems security and privacy. They are used as an intellectual framework; the framework offers guiding principles, strategy and concepts to bring about a coherent approach as well as collaboration effort and systematic move towards lasting solution (Kenneally, 2009).

2.2.7.2 The Anonymisation Trace Problem

The problem with trace anonymisation is a broader area than simply preparing traces for public data. Some organisations require anonymisation of any stored traces, even if stored internally. This can require online anonymisation, which can introduce complexities. However, offline anonymisation bears new challenges directly impacting privacy of user's information. Furthermore, in order to retain research value in the traces, the policy ended up requiring a multi-pass structure. While online anonymisation can leverage some of the techniques outlined in this research, its possible new development may seek system to system anonymisation without human interference remains an area for future work.

In order to carry out our daily routine activities, we shop online, use out private life gadget and technological means of payment to the goods and services, hopping that life has become easier with transactions and busyness at out finger tips. On the contrary, data we release are automatically stored, filtered and monitored before being passed to third parties for advertisement and business marketing strategies online. This can be seen as

bridge of trust, braking of rules of law to confidentiality and data protection. Nowadays, computer applications software is designed to trace identity and privacy crack of users.

According to Gong (2014), while we enjoy easy payment method to our bills and household monies, we use our debit and credit cards as means of method of payments. Consequently, these cards carry our data such as date of birth, postcode, and surnames which are re-entered to confirm identity, then the data is stored and shared to other organisations (Xie, et al., 2006).

While doing such activities we leave behind a significant data trail accessible for internet surfing on the same website, other users might have access to. Therefore, privacy policy is violated, human personal capacity and privacy is interrupted and life and social activities are limited as there seem to be in adequate freedom to single life (Xie, et al., 2006).

Data transfer requires balancing in facets of privacy, security, and legitimate benefits (Bynum, 2003). Anonymisation of data can reduce the risk privacy policy and legal desires. However, counter measures negotiation recent anonymisation systems can uncover secure data in released datasets (Kenneally et al, 2010).

2.2.8 Distributed Systems

The distributed systems comprise of several interconnected autonomous computers, linked together via network tools and middleware to allow their coordination as well as the sharing of the system resources. The users of the distributed systems see it as a single

computing facility that is integrated. One of the goals of using distributed systems is to make the resources accessible for the users (Tanenbaum & Steen, 2002).

However, it has a goal to create distribution transparency to the user in terms of location, relocation, access, migration, failure, concurrency and replication. Another goal of the use of the distributed systems is to create openness and scalability. Basically, there are three types of distributed systems, namely the distributed embedded systems, distributed information systems and the distributed computing systems (Beekhuyzen et al., 2003).

The distributed computing systems are used for the tasks with a requirement for high-performance capabilities, and it comprises sets of personal computers or similar workstations. The classification of the distributed systems is oriented towards the support of information processing, pervasiveness, and computation.

The distributed systems architecture is achievable via several configurations under such styles as layered architectures, data-centred architectures, object-based architectures and event-based architectures. The system architectures of the distributed systems take both the decentralised and the centralised organisations (Jia & Zhou, 2005). However, the most important organisation is the client-to-server architecture, where the software allows a set of machines to function in a natural distribution. Another important organisation is the peer-to-peer systems that allow the organisation of processes via an overlay network. As an integration of software and system architectures, the self-managing systems have emerged, and they are organised as loops with monitoring components to provide feedback control.

The distributed systems apply several processes as the basis of inter-machine communication. One of the processes is the threads, and they allow the use of the CPU after the blocking of the I/O operation. Another set of processes is the client processes, which allow the user interfaces' implementation in the range of simple-advanced implementations to handle all ranges of documents. The server processes are more complicated than the clients' but can either be stateful or stateless, concurrent or iterative, can implement at least one services. The distributed systems also involve code migration to help increase flexibility and the performance of the components of the distributed systems. In this paper, the understanding of the principles and approaches of implementing distributed systems provides the basis for the identification of the risk areas of the users' privacy and information security (Google and UK Call a Truce on Privacy Policy' 2015)

One of the practical use of the distributed systems and networks is the concurrent programming. Concurrent programming allows programmers to use a single CPU to execute an application without the locking out of the I/O operations. For the concurrent programming, a specific program contains at least two processes working together in the performance of a specific task. The concurrent program processes work by intercommunication with each other in a synchronised manner. By the use of the interconnection network, memory modules and the processors are linked to form shared-memory multiprocessors. The reason behind the use of the multithreaded programs is the ease of organising the data structures and the codes as a set of processes (Andrews Gregory, 2000).

2.2.8.1 Privacy in Distributed Systems - Limitations and Problems

The distributed systems experience a few privacy limitations that makes the make the businesses find the use of the centralised systems more preferable for business activities. In the mobile distributed systems, the ability of the users to use mobile devices is created by context awareness. However, there are a number of limiting challenges, one of which is the limited preservation of the user's privacy. Even though numerous approaches of user-aware modelling contexts are available, the preservation of the user privacy is always a challenge. However, the privacy can be observed via context-aware modelling with an extension of the unified modelling language.

In the distributed systems, the privacy is threatened by the low levels of information security. Unlike the centralised systems that offer the ease of data control, the distributed databases allow the data control from multiple locations is creating multiple chances of information security breach across the network and the consequent privacy violation (Bellamy, and Raab, 2005). Even though there has been a high level of improvement in the network security management and technologies, there is no ultimate attack immunity in the technological products and the existence of a network creates high chances of privacy issues. However, the distributed systems have very high levels of intricacy because of its capability of to replicate the data. Consequently, the software failure can lead to a lack of reliability and performance in security-challenged situations (Simons & Wirtz, 2007).

2.3 Privacy and security

Security is related to privacy in a simple connection where the protection of the information privacy makes it a necessity to include security (Chander, Gelman & Radin, 2008). However, the relationship between privacy and security requires balancing through policy. In computing, the policy describes the right to the information access, and it is aimed at bringing the protection of the information integrity and confidentiality. On the other hand, the term security as applied in computer systems describes the protection data, information and resources from the unauthorised usage (Nabeel, 2013). The security's main focus constitutes the access to information, data and resources. On the other hand, privacy regards to the storage of personal and private information, as well as to its appropriate use (Karat et al., 2009).

Just like privacy breach, information security breach is also highly costly. One of the costs of information security breaches is economic. For the corporate entities, the breach to financial and other sensitive information has various levels economic implications whenever the prevention of such breaches happens. Most security breaches are reported in the newspapers if the details ever enter the public domain. The o security breaches via the unauthorised access relating to financial information elicit a more significant market reaction as compared to that related to the unauthorised access to confidential information. According to Campbell et al. (2003), the stock market provides a good record of the economic cost of information security breaches. Most financial journals and newspaper report the financial loss caused to the companies after information security breaches. Upon announcement of a company's involvement in the information breaches, the market reacts in different ways to that company, and the economic performance of its

future is negatively impacted. If the information security breach includes confidential information, the impact is even more pronounced. However, such breaches as a denial of service do not have many adverse economic impacts on the victim, and the market does not react much badly because of their less connection to the firm's economic performance (Newman, 2015). Privacy of the firms' information only remains intact if the company does not experience security breaches. Similar to the information security breaches, privacy breaches also have economic impacts on the owner company (Wang and Kobsa, 2013).

However, Campbell et al. did not draw a relationship between the economic implications of security breaches to those of the privacy breaches in the company (Campbell et al., 2003).

In the distributed systems, information security and privacy issues are highly unprecedented. However, these issues cannot justify the end of the use of the distributed systems because they offer high levels of beneficial features like reliability, expandability, efficiency and manageability. The security and the privacy vulnerabilities of devices of the distributed systems result from the high levels of inter-connections. Cao et al., 2014, highlight various work related to the privacy, trust and the security of the information. In their work, they are able to assess various models of improving information privacy and security of the systems to increase the trustworthiness of computing applications. Among the papers considered is the first group that examines the ways, tools and methods, as well as the issues related to trust in the use of the interconnected systems (Matherne and Mackler, 2002). The second group addresses the privacy issues related to the use of, methods and techniques used in the interconnected

systems. The papers highlight the benefits of the certificate less anonymous systems of remote authentication in allowing the users enjoy privacy in health care service provision. However, the traffic masking algorithm is discussed in detail, together with the costs of the use. Most of the papers discussed deals with the security of the distributed systems where different issues, from data recovery methods, intrusion prevention and balance between privacy and security, amongst others, are addressed (Cao et al., 2014).

The health care service sector is one of the most receptive to the use of technology. Most of the machine systems in the hospitals are interconnected. However, the information generated by the health care fraternity is rated among the most confidential because it relates to the intimate values of the clients. In the US, the health information privacy and security is regulated under the HIPAA regulations (Campisi, 2013).

However, the amount of pressure mounted against these regulations is high because the use of IT in the healthcare service provision is capable of providing the protection to privacy but it leads to the magnification of the associated risks (Li, 2003). The CDT paper, 2014, provides an in-depth examination of the success variables of a complete information privacy and security in the health care systems. According to the paper, the frameworks of ensuring information privacy and security depends on three factors that include the implementation of the principles of privacy, the adoption of the trusted characteristics of network design and the establishment of the mechanisms of accountability and oversight (cdt.org, 2014).

The paper observes that there is no specific method of ensuring a policy meets all the privacy and security needs. However, privacy can be achieved to greatly high levels by

adopting a framework that has various specific attributes to ensure all the aspects of the concepts get redress. One of the basic characteristics of the framework that improves the information and privacy situation in the health care setting is the limitation of the data use to the authorised parties. However, another attribute is the data collection limitation to avoid landing to the unauthorised parties (Gandy,2003). Other attributes of the framework include the security controls, data integrity as well as oversight and accountability. In the health care context, the role of the HIPAA is to provide the legal-ethical guidance in the development of health care systems with capabilities of providing high levels of information privacy and security integrity (Miyazaki & Krishnamurthy, 2002). However, the availability of the clients' consent to the health care information use, privacy and security of the information is more sophisticated and requiring highly multi-variable approaches of use (cdt.org, 2014).

2.3.1 Privacy and Software / Hardware

2.3.1.1 Privacy and Software

For the privacy standards-aware software, their design prevents the distribution of personal information for commercial uses (Tynan, 2005). However, the privacy invasive software ignores the privacy of the user and distributes the personal information for commercial uses. The privacy-invasive programs come in three classes, namely spyware, content hijacking software, and adware. The software privacy invasions involve several internet usage aspects (Micheti, et al., 2010). The spyware invades privacy by secretly collecting and distributing the information for the system user. On the other hand, the

adware invades the privacy of the user by creating displays of advertisements in the system depending on the information gathered by the spyware. The keylogging software saves a record of the keystrokes of the users with the intents of monitoring the behaviour of the system user (Deswarte, 2004). The data-harvesting software invades the system user's privacy by gathering the contact addresses with aims of spamming them at later dates (Laudon & Traver, 2013). The spyware software has considerably changed to include several sub-categories such as trackware, badware, thiefware and scumware (Keizer, 2012).

The badware has two basic characteristics. One of the characteristics of the badware is that they act irreversibly or deceptively. The second characteristic is that they portray objectionable behaviour.

2.3.1.2 Privacy and Hardware

Privacy violations can be as a result of physical security breaches. The most appropriate physical redress to the physical security issues of the information systems is the use of the physical barriers. However, the protection software aspect of the information systems, physical protection applies to the physical equipment and terminals as well as the removable hardware like punch cards, printouts, tapes and other data storage devices (Klosek, 2000). The physical protection of the terminal functions to restore information privacy via the prevention of visual inspection of the information components. It also restores privacy by the prevention of entry of the unauthorised individuals. Moreover, it offers the protection to the terminal against tampering. The physical protection of the data

is achievable via three specific guidelines. One of the guidelines is the securing of the computing devices as well as the equipment to avoid the disruption of the sensitive aspects of the systems (Council of Europe, 2002). The second guideline is a continuous protection of the critical computing equipment to mitigate the risk of the physical threat. The third guideline is the physical protection of the remotely located terminal devices to avoid physical security breaches that would compromise the data privacy.

2.4 Privacy Frameworks

The last half of the twentieth century presented with marked digital technological advancement as well as numerous undeniable benefits. However, the technologies have caused revolutionary setbacks to the personal privacy of the consumers. However, the technological development rate was more pronounced than the adaptation of the regulations, federal laws, standards and the best practices of the industry in relation to the technologies. However, the US government was able to respond to the privacy implication of the digital communications by erecting regulations for monitoring the use of the data with privacy implications. In that response, it has provided a framework for the privacy protection without disfavouring the global digital economy's innovation. The framework addresses the concerns of the consumer privacy in the light of the commercial use of their information (Almeida & Poell, 2012). Such aspects captured by the framework include transparency, security, the individual control as well as accountability, amongst others.

With regard to the online privacy, the framework aims at allowing efficient monitoring of the uses of the personal information by the commercial entities. Additionally, it aims at reinforcing the appropriate disclosure of the personal data by the companies on the basis of the most consistent context (Thierer, 2013). The framework also provides the description of the personal data in the context of privacy for both online and the offline contexts. Since the online gathered personal data is used for the advertisement purposes, the framework highlights the aspects of use that discourage the compromise of the personal privacy. Almeida and Poell (2012) through their analytical paper highlight the challenges posed by the government's standards for the use of the personal data for commercial purposes in the search for privacy and innovation balance use of the digital technologies (Almeida & Poell, 2012).

The use of the video surveillance technologies poses numerous challenges privacy. It is highly difficult to maintain privacy in the management as well as the processing of the live videos and thus calling for the application of an efficient framework to prevent the associated risks to the privacy. For the live video use, management and processing to observe efficient levels of privacy, the three significant variables require high levels of consideration. One of the variables is the supportability of the software system to the ad hoc monitoring tasks. In this variable, the domains related to the monitoring tasks are redressed (Anton, et al., 2011). The second variable is the provision of the capabilities of enabling the fast development of the custom applications to address the problems of domain-specific users. The third variable of the framework is the high levels of need for personal privacy as well as the levels of pervasive monitoring' objections. A software layer for live video management and processing has three levels. One of the levels is the

camera adapter. This level includes five activities that revolve around image streaming. The five activities entail privacy handling, image analysis, object detection, communication handling, and frame-to-frame tracking. The second level, the spatial processing layer, deals with the images descriptors' streams. It also includes five activities. These activities include communication handling, privacy management, indexing, camera session management and spatial queries. The third level includes steam processing, and it has five activities, namely communication handling, client session management, query execution, stream processing, and notifications. The camera use in the multimedia systems include such areas as healthcare, environmental management, battlefield visualisation as well as urban surveillance making it a target factor in the digital privacy framework, and the management of the live video databases (Aved & Hua, 2012).

In Saudi Arabia and across the globe, privacy is a high-interest cultural value. It is this level of regard that makes it a universal practice to create forts in homes across the entire globe. However, being a major reflection of almost all cultural groups, privacy is also reflected in various laws. In the Arabian legal environment, privacy right is a provision that derives its standing point from the dignity of an individual. As expected, the legal provisions of privacy are enshrined in the constitution hence guaranteed under constitutional frameworks. The legal framework of privacy in this Middle East country has around two principle factors that address privacy. One of such factors is the tort claim – masouliya taqsiriya (deficient in responsibility). Through the masouliya taqsiriya, one can claim for damage compensations after the wrongful disclosure of the personal information. This tort claim has a basis in the data-related laws related to the technology and information industry's privacy violations. The legal references of this tort claim can

be located in the art. 37.13 And art. 37.7. of the Saudi constitution. The second legal factor is the Anti-Cyber Crime Law, 2007. This law is prohibitive of the interception of or the infiltration of personal data. That notwithstanding, the legal perspective of privacy in relation to the Saudi law is still in the development phase and cannot be applicable in the legally developed contexts like the US (Balouziyeh & Hussein, 2012).

2.4.1 Developing Privacy Policy Frameworks

In distributed systems, remote authentication is a common technique on the basis of three factors, namely biometrics, smart card and password (International Conference on Information Systems Design and Intelligence Applications, & Mandal, 2015). For the distributed systems with two-factor authentication, a lot of benefits can be seen if the upgrades are made to the three-factor authentication. One of the benefits of such upgrades is the improvement of the privacy of the users. A privacy framework for such an upgrade should be custom and secure (Kadloor, et al., 2012). The framework's first factor includes codes known by the clients to access the services or applications in the system. The first factor approach to authentication has lower entropy and encourages privacy attacks through such practices as phishing. The two-factor authentication includes the use of the first factor followed by a second factor, a hardware token, of authentication to access the service or program in a system. Finally, the third factor authentication includes a biometric authentication factor on top of the code and the hardware factors of authentication. Although the third-factor authentication offers high levels of information privacy, the biometric features used for authentication cannot be concealed. The third-

factor authentication framework serves to ensure data privacy because of the lack of tolerance to biometric factors data errors (Huang et al., 2011).

For the development of the privacy framework to be a successful endeavour, there is a need for the consideration of various variables, namely privacy, data flow, confidentiality and the framework development processes. With respect to data privacy and confidentiality, various legal requirements affect the considerations made. Different regions will have different legal shades for the support of privacy through readily established policies. In the standard diagrammatic demos, the framework is represented via standardised notations to show the Privacy ad policy requirements, data flow requirements and the privacy enhancing techniques, as well as the allowance for the privacy threat analysis. Kuchinke et al. 2014, described the diagrammatic framework to cover three zones of privacy for a health care context, namely the research zone, care zone and the non-care zone. The Kuchinke et al. 2014 model of the diagrammatic description of the data privacy frameworks allows for the adequate, structured analysis of the privacy and the confidential issues of the patient's data. However, it also allows the framework specification for data privacy communication requirements, and data flow privacy compliance and the identification of the data privacy implementation weak points. However, this model is limited for use in the healthcare industry (Kuchinke et al., 2014).

2.5 Structuration Theory

The structuration theory describes social life as a composition of more activities than just the random individual acts (Putnam & Mumby, 2014). However, it adds that it is also a

product of more than just the social forces. In simpler terms, social life cannot be fully described by either the micro-level activities or the macro-levels activities. In a suggestion, the theory sees the social structure and the human agency as an association of each other in which the repetition of the human acts generates the structure. The theory observes the social structure as a matrix of institutions, traditions, moral codes and the cultural practices. This matrix, according to the theory, is subject to change as a product of differential reproduction, ignorance, and replacement.

The theory describes the human agency as the transformative capacity. The transformative capacity is the power that allows the humans to exploit the existing resources. The resources, the theory observes, include the structured social systems' properties originate from the knowledgeable agents during the interaction (Haftor, Mirijamdotter & Bradley, 2011). According to Giddens, a structure is a product of the resources and rules involved in the social reproduction. A structure can be seen in two lenses of rules, namely the codes of signification and the normative elements. Structure exists in duality, with such dimensions as modality and interaction. The elements of the structure involved in the duality function include domination, legitimation, and signification. Modalities of the structure include norm, interpretative scheme, and facility. The elements of interaction involved in the structure include power sanction, communication and power (Molloy et al., 2008).

Even though the structuration theory has a few conceptual shortcomings and is powerful for eliciting social understanding, the theory has a few limitations in its applications in the fields of computer science and information systems (Jones and Karsten, 2003). Additionally, the information systems practitioners and researchers ought to work with

the theorists otherwise the significance of the theory of computer systems development would lack (Spierings, 2014). Moreover, the theory does not have models to follow making it difficult for the bridging of the practical and the theoretical aspects.

2.6 Related Work

Anton et al. (2011) consider the increasing rate of development of ICT, and the fact that more people both at home and in the workplace are engaged in activities such as online shopping and banking, has led to an increased risk in terms of violation of privacy and anonymity. The reason for this has been that there are disclosures of sensitive information which has led to the misuse of data, therefore, there is a need for developing a technique for identifying and documenting privacy requirements that are easy to implement (Anton et al., 2011). To overcome these issues Anton et al. (2011) recognise the fact that consideration of privacy should not be an afterthought and should not be ad hoc and that users should be able to understand their privacy policies and what happens to their data. While this is right approach and agrees with the principles of the present study, the approach suggested by Anton et al. (2011) does not seek the opinions of users and does not consider privacy perception.

Writers that do consider privacy perception are Paine et al. (2007). In their approach to the issue of privacy they try to understand the privacy concerns of people using DS and even try to understand the reasons behind those concerns, however, they fail to fully define these privacy concerns and they do not apply their findings, their findings are form information purposes only and they do not extend beyond understanding privacy towards

a solution in DS. Moreover, Paine et al. (2007) make no reference to the technological implications of privacy.

Calo (2011) delve deeper into the issue of privacy and consider both the subjective and objective considerations of privacy, the present study does this by looking at the subjective views of the users and the objective aspects of privacy from the technological considerations. However, a limitation of Calo's (2011) study is that although he has a deeper understanding of privacy perception because there is an acknowledgement that there is privacy harm even if there is no privacy violation, the ideas do not consider the technical aspects of privacy and importantly, do not apply the principles into a framework that can contribute towards the development of privacy policy.

Rubel and Biava (2014) present a framework for analysing and comparing privacy states, they employ a method that precisely describes privacy using a lexical approach through the use of flexible vocabulary. Importantly, relevant to the present study, it links conceptual and philosophical ideas about privacy with social sciences and work on privacy policy. The approach is open to the different concepts and nature of privacy and approaches privacy as a real world issue, and importantly, considers privacy together with context. In reference to the present study, the context is something that is very important, and the very open and nuanced approach to the concept of privacy using language descriptions is also something considered in the present study. However, Rubel and Biava (2014) make no reference to the application of their ideas to the technical considerations of privacy such as the development of privacy policy for distributed systems.

2.7 Summary

In summary, this chapter presented a review of the literature related to areas that are relevant to the study. Primarily, the study is concerned with privacy and the perception of privacy of users of distributed systems, accordingly, literature was reviewed about privacy its meaning and how it is perceived with an emphasis on the types of information that are considered private to users. Moreover, because the study is concerned with disambiguating privacy, this area was also addressed. The main idea behind the present study is to create a framework that is based on two areas; firstly, the technical considerations for privacy in distributed systems and secondly' the perception of privacy of users of the systems. In light of this approach of the framework, it was necessary to consider privacy in relation to software and hardware and specifically in relation to distributed systems. Finally, as the present study proposes a privacy policy framework, existing frameworks were reviewed.

Chapter 3

Methodology

Objectives

- Presents the methodological approach and the research methods that are employed.
- Theoretical foundations for the methodology and the use of questionnaires and interviews.
- Particular attention to paid to how the research instruments contribute to the aims and objectives of the study.
- How the research is conducted, the sampling and the ethical issues are addressed.

3.1 Introduction

This chapter presents the methodology to investigate and analyse current approaches to privacy policies and the associated technology and to gain the perceptions of privacy that will be used as part of the proposed framework of the study. There is an explanation of the theoretical foundations behind the methodology and justification for the chosen methods in relation to the aims and objectives of the study.

Surveys are conducted with users, developers and owners in order to determine whether in an enterprise where privacy is considered a high priority by employees, owners and users are satisfied with the way their private data is being handled and if they encountered any issues when data exchange takes place. Moreover, the research aims to understand the current situation as regards privacy policy and the associated technology and to gain an understanding of the perceptions of privacy. The survey was divided into three parts; first, an expert survey semi-structured interview conducted with experts. In this a set of questions were used to gather information about privacy before applying the PPF framework. Secondly, a questionnaire was conducted with the users and developers of distributed systems. Thirdly a post PPF questionnaire for evaluation purposes was conducted with all three groups.

The reason behind the post PPF questionnaire is to evaluate the PPF framework and to develop a construct to assist in building recommendations to users and developers of distributed systems. Moreover, this questionnaire was designed to enable the research to determine the impact of applying the PPF framework among users, developers and owners.

For study it was important that the research obtained first-hand data from the participants, in order to formulate rational conclusions and make recommendations. Two important aspects of the descriptive approach are that it is quick and practical in terms of the time and resources required. The selected participants answered a survey questionnaire designed in the descriptive method format, with both closed and open-ended questions. Data gathered from this research was then computed for analysis.

The survey instruments employed in this study aimed at collecting data from key users of enterprise distributed systems including developers, users and owners; in addition to government representatives.

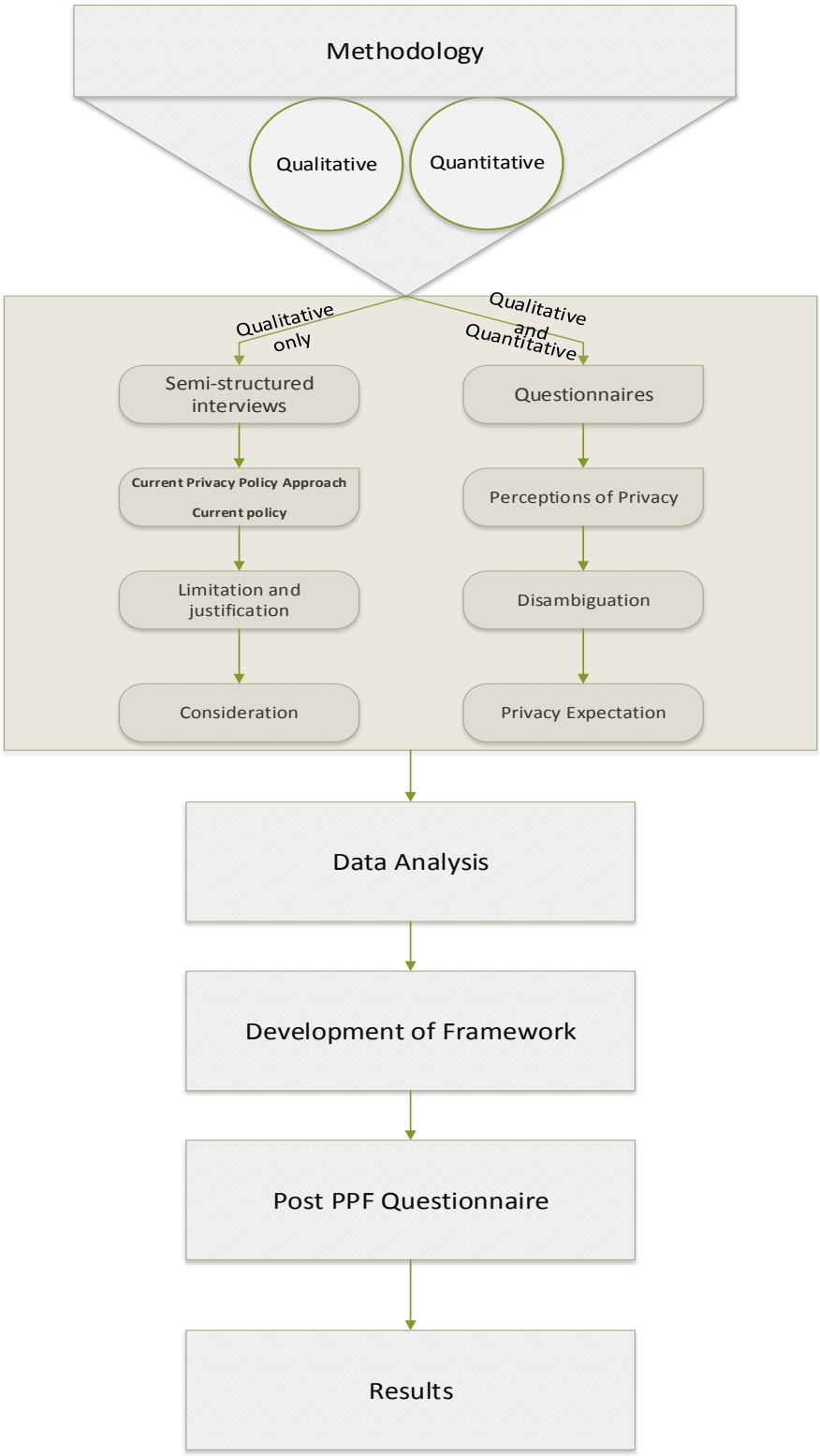


Figure 3.1: Methodology Framework

3.2 Theoretical Foundations and Methodological Approach

The theoretical foundations behind the research methodology are presented here together with the methodological approach which has been selected in order to achieve the aims and objectives of the study. As shown in figure 3.1 in the above, the methodology used both quantitative and qualitative research in the form of questionnaires, both qualitative and quantitative research, and semi-structured interviews for qualitative research. The semi-structured interviews are used to gather data about current privacy policy to provide a justification for the proposed framework and the questionnaires are used to gather data about perceptions of privacy. Towards the development of the proposed framework the data is then analysed. The post framework questionnaire is used to validate the proposed Privacy Policy framework.

3.2.1 Descriptive Approach

The present study adopted a descriptive approach. Studying the extremes of human experience, studies about creativity have found that conceptualisation involves more than simply relating words; knowledge also includes conceptualisation of scenes, rhythm, sequential ordering, values and identities. In defining descriptive research is a method of research that gathers information about the current existing condition.

Therefore, a descriptive method of research was used for this survey. The reasons behind selecting this method are as follows:

1. To determine the factors of success/failure in relation to technology and privacy.

2. To establish the factors of success/failure in relation to knowledge and skills.

Success or failure constitutes one of two dimensional arrays that this survey will cover; the first dimension is the technology factor – what is permissible in terms of technology - and the second dimension is the human factor, represented by perception of privacy.

The aim of conducting out a descriptive survey was to establish the factors for success or failure in relation to privacy of the technology and the client and to find out if there are other reasons that determine enterprise privacy policy success or failure. The descriptive approach is practical, quick and flexible so that when important issues that need to be addressed arise, further investigation can be carried out. Descriptive research is mainly concerned with describing the nature of a situation as it is at the time the study takes place, and to discover the causes of a phenomenon. The method can use a quantitative or qualitative approach which allows the research more options in choosing the appropriate research instrument.

3.2.2 Quantitative Research

The aim of quantitative research is to derive measurements that are valid and they can be generalised easily anticipating cause and effect. Being quantitative research is specific in nature it depends on formulating research hypotheses which are then confirmed empirically using a data set. This approach is more focussed on the detailed description of a phenomenon. Therefore, the researcher's subjective personal thoughts and biases are not appropriate to this method.

Quantitative data-gathering instruments establish a relationship between measured variations and the researcher is often detached from the study and the final output is free of context. Therefore, the researcher does not interfere with the process or the outcome of the surveys. The measurement, statistics and numerical data are the main components of quantitative research instruments. With such research instruments, a detailed description of data collection and analysis is necessary for trace back and following on by other researchers.

In the present study quantitative data collection methods, specifically, questionnaires are centred on the quantification of information related to current privacy policy, technology and privacy perception. This was mainly to show the variations between the user's knowledge of privacy, and programmers' understanding of users' and owners' requirements in relation to privacy.

3.2.3 Qualitative Research

The aim of qualitative research is to develop concepts which assist in understanding social phenomena in natural settings, emphasising meanings, experiences, and opinions of the participants. It is safe to conclude that the underlying concept of qualitative research is a trend seeking state as opposed to quantitative research which is the current state of a given phenomenon.

Qualitative research generates verbal information instead of numerical values. The qualitative approach uses content or holistic analysis to explain and understand the findings through inductive and not deductive reasoning.

The aim behind using qualitative analysis in this research is to be able to investigate user cognition and perception of privacy. A qualitative approach helps to identify and investigate users' perception to better understand the meaning users have constructed about privacy within the traditional approach to privacy policy, meaning how privacy is handled within organisations. The overall focus is on finding out how users make sense of privacy based on experiences.

This derived qualitative data can not only be used towards the development of the PPF, but also towards the development of automated privacy settings that allow a privacy choice through a privacy button on the keyboard, one of the main contributions of the present study.

In reference to the present study, the high variability associated with cognitive and perception issues that may vary considerably among the participants can be considered by a qualitative approach. These variations may occur for different reasons such as language, memory ability or skills.

3.2.4 Structuration Theory

The everyday actions of people reproduce and reinforce a number of expectations and it is these expectations which comprise the 'social forces' and 'social structures'. According

to Giddens, 'Society only has form, and that form only has effects on people, in so far as structure is produced and reproduced in what people do' (Giddens & Pierson, 1998: 77).

These ideas can be related to privacy expectation, the human actor is being asked what privacy really means, and the result is a privacy policy (structure) that is based on these expectations. Current structure (current privacy policy) needs to be replaced or reproduced differently.

Existing privacy policy (structure) was written by a person (human agent) but now the human agents (users) are changing and their perception of privacy is different, therefore, the agent is now changing the structure (privacy policy) – because social structures which include established ways of doing things/codes (privacy policy) can be changed when people start to ignore them, replace them or reproduce them differently. The actions of the human agents (users' privacy perceptions and expectations derived through interviewing etc. and the privacy button) will change the approach to privacy policy (structure within which users operate in terms of privacy).

The main research question of the present study is as follows: 'How can distributed system architecture be combined with a structuration theory approach for privacy disambiguation?' This question can be answered by understanding that perceptions of privacy is a social phenomenon and that within social sciences there are two main approaches, namely; the subjective and objective, to understanding such phenomenon and the structuration theory aims to utilise and combine these approaches. Specifically, there are those who see social phenomena (things that happen with people) as people interpreting or viewing their experience, what is happening around them, subjectively, in

other words action is based on subjective interpretation of world around people (Jones, 2003). Alternatively, there are others who see social phenomena as result of influences of objective social structures, in other words action is caused by objective things that are external to the person. Giddens says that towards understanding these social phenomena these two approaches should be combined and considered together at the same time (Jones, 2003).

3.2.5 Mixed Methods Approach

The study adopts a mixed methods approach by utilising both quantitative and qualitative approaches towards deriving privacy perceptions and to test the developed and implement the PPF. The benefits of using a mixed methods approach is that include that the issue can be addressed at different levels,

Data in Table 3.1 shows how the qualitative and quantitative approaches are used in conjunction to determine technological and human factors. These methodologies take into consideration success/failure aspects of privacy policy implementation, and bind those to a particular enterprise services.

Dimension	Surveyed	Survey Method	Relationship
Technology Factor	Owners	Expert Survey (Qualitative)	E2E/O2E
Human Factor	Users	Questionnaire Survey (Quantitative)	U2E/E2E/E2O

Table 3.1: Qualitative and Quantitative Methods

3.3 Research Methods

The research methods adopted in the present study are semi-structured interviews and questionnaires, the former forming the qualitative side of the research and the latter forming the quantitative side. Here these methods are presented together with a justification for their adoption, how they are developed and how they are deployed. It was important that the research instruments assisted in eliciting perceptions of privacy and also elicited opinions about the idea of the new framework for privacy.

Interviews were considered for the research in order to derive data about the current situation regarding the distributed system and more specifically, information regarding the current privacy policies and the perspectives of those responsible for managing their implementation. For interviews there are three main approaches; structured interviews, semi-structured interviews and unstructured interviews. As regards structured interviews they have a rigid set of questions that although allow the research to address the areas according to the aims of the study, do not allow the interviewee to speak more freely and do not allow the interviewer the flexibility to probe into issues as they arise, both of these limitations may lead to a narrow representation of the issue being investigated. At the other end of the scale, unstructured interviews would resolve the issue of allowing interviewees to elaborate on responses and the interviewer to probe further, however, because they are based on the idea of a free flowing conversation and there are not pre-set questions, each interview may be completely different to the other which would affect the reliability of the interview as a research method, moreover, this type of interview may require the skills of a trained interviewer and can be time consuming. Therefore, it was decided to adopt the semi-structured interview format because it provides the structure

required for reliability and the flexibility to allow opinions and perspectives to be revealed.

3.3.1 Semi-Structured Interviews

A semi-structured interview is employed in this study. The interview contains a list of questions and the interviewer allowed the interviewees to clarify any vague statements they made for further elaboration. The interviewer attempted to remain objective and tried not to interrupt or influence the interviewee in any way.

The idea behind the questions in the interviews with the experts was to ascertain the current situation as regards privacy. The questions were as follows:

- Do you feel privacy policies you have available in your organisation allow you to serve users best?
- What U2U services does the enterprise provide with respect to privacy?
- Describe how the information systems that support this service?
- Describe the privacy issues concerned when delivering this service and how the privacy policy (if it exists) is evaluated?
- Are other outsourced companies providing a privacy policy for the enterprise?
- Are your enterprise privacy policies accessible to users with special needs?

The semi-structured interview, much like the focus group, is an orderly or partially structured way of talking to people to gather information and involves paying attention to what people say and being judgmental (Longhurst, 2010).

One of the main benefits of semi-structured interviews is that because the interviewer does not adhere strictly to a fix set of questions there is flexibility for respondent to elaborate on responses. Specifically, the semi-structured format allows the interviewer to probe deeper or seeks further clarification on any issues or ideas raised by the interviewee. According to Gillham (2000) using open questions does not necessarily mean there is no control over the way the interviewee responds and there is a need for unobtrusive control in order to steer the direction of the interview to ensure the key points are covered towards achieving the aims of the study. This is achieved through the use of prompts, these can be considered during the development of the interview questions, and additionally the interviewee is able to seek clarification on points raised by the interviewee (Gillham, 2000).

The semi-structured interview was considered relevant to the present study because part of demonstrating the application of the framework is to disambiguate the meaning of privacy which is translated into privacy expectations, and to derive the technical considerations that are relevant to the development and implementation of privacy. These technical considerations are expected to include the architectural constraints and organizational technical requirements that have an impact on privacy policy. Therefore, there is need to derive opinion and to allow respondents to explain how they feel about privacy and talk freely about the technical issues of distributed systems that relate to privacy policy. The issue of privacy is something that is very personal and subjective and

the only way to elicit and understand these opinions is by allowing respondents to talk freely, hence the choice of semi-structured interviews.

3.3.2 Development of Interview

It is first important to note that because of the aims of the study the interview will be qualitative and therefore, flexibility is a key aspect of qualitative interviewing (King and Horrocks, 2010). Thus, the development of the questions considered that both the participant had to answer questions related to the topic and that any issues that emerged during the interview could be probed further.

In line with the aforementioned principles of the semi-structured interview, the development of the interview schedule is based on the idea that it is a guide to the issues that need to be discussed and is not asset of fixed questions. Specifically, the questions will allow for a conversational manner to develop (Longhurst, 2010). In a semi-structured interview the interview guide should include an outline of the topics that need to be covered including suggested questions (Kvale, 2007).

The interviews were conducted with the senior management of the respective organisations for two main purposes; firstly, to determine at the overall organizational strategic level the current situation for privacy policy and secondly; to disambiguate the meaning of privacy for senior management. This is useful to show if there is a difference between the strategy for privacy that they initiate and their subjective perception of privacy, this is justified by the fact that one of the main motivations for the present study

is that all too often privacy policy is established as a technical policy and does not consider the subjective perceptions of privacy.

3.3.3 Piloting

There is a lot more to interviews than simply asking questions, there is a need to get the management of the interview right and to practice and pilot the interview to make last minute alterations and adjustments (Gillham, 2000). The semi-structured interview was piloted by conducting an interview with senior manager at the Northern Cement Company and a senior manager at the Technical and Vocational Training Corporation. According to Gillham (2000) it is important that those used in the pilot are representative of the group that is being researched. The pilot study was carried out determine the clarity of the questions and to see if they elicited responses related to the topic at hand.

3.3.4 Sampling for interview

In quantitative research a sample is chosen that is statistically representative of a population that is being studied to establish generalisability from the results (King and Horrocks, 2010). In contrast qualitative research does not try to make this generalisation and thus does not use sampling strategies that are designed to produce statistical representativeness; however, it is also important that the sample relates to the phenomena that is under study (King and Horrocks, 2010). Therefore, in light of these ideas a total of 10 senior managers who fit this criterion were sampled from the three organisations, 3

from Al Rajhi Bank, 3 from the Northern Cement Company and 4 from the Technical and Vocational Training Corporation. The interviews were designed to elicit responses from those at the highest level of the organisation responsible for the overall strategy for distributed systems and the associated privacy policy.

3.3.5 Conducting the Interview

The duration of the interviews was approximately one hour and they were conducted on the respective company premises. The prospective interviewees were asked where they would like the interviews to be carried out and all of them said they wanted the interviews to take place on their premises. Privacy was an important consideration for the research, it is important that there are no interruptions and the phone has to be switched off (King and Horroacks, 2010).

The interviews were conducted in English and were audio recorded. It was ensured that the interviewees were familiar with the recording technology and tested the equipment in the room before conducting the interviews (King and Horroacks, 2010).

3.3.6 Interview analysis

The audio recording were transcribed and the fact that transcription could be an interpretative process because of the differences between written texts and oral speech and that there is a translation from a spoken language to a written language was considered (Kvale, 2007). However, these issues are partially overcome by the use of

audio recording, nevertheless, things like the tone of voice or pauses are lost in the transcription (Kvale, 2007).

Because one of the objectives of the interview was to elicit the meaning of privacy there was a need to focus on the meaning rather than the linguistic form (Kvale, 2007), this was achieved through content analysis which involves the coding of a texts meaning into categories so that the frequency of specific themes can be identified (Kvale, 2007).

3.3.7 Qualitative Analysis

There are three broad approaches to survey data analysis: Interview, written data and observational approaches. Interview and written data are relevant to the research problem in hand. Interview results are analysed and organised in categories corresponding to the measured success/failure factors. They are crucial when conducting qualitative analysis; the research also depended on top enterprise officials' feedback to be able to build a strong case for the research argument; this was in addition to the findings from the written survey.

3.4 Questionnaires

It is important to note that there were two main objectives behind the questionnaires, firstly, (objective 1) to ascertain the current situation as regards current privacy policy and the current technical situation of the organisations, the latter helping to inform the technical side of the lexica-technica construct, and secondly (objective 2), to derive

privacy perception from the parties which formed part of the framework itself i.e. the part of the framework where privacy perception is derived contributing to the lexica side of the lexica-technica construct. Again, as with the semi-structured interviews, the reason for finding out about the current situation and the perceptions of privacy is to see if there is a difference between the two towards a justification of the study. In others words if the current approach to privacy is different to privacy perception then the current approach is redundant in terms of addressing the privacy needs of users.

3.4.1 Development of Questionnaire

The questionnaire was distributed to users and developers of the distributed systems. The questions were designed to answer questions related to techno-social aspects, privacy attributes and knowledge.

During questionnaire development the first objective of the questionnaire was to ascertain the current situation as regards the success or failure of current privacy policy and the current technical situation of the organisations from the perspective of the employees, of one public and two private organisations. Specifically, this included establishing their level of satisfaction, their ideas and the requirements.

These objectives of the questionnaire are designed to address the overall objectives of the study. Therefore, in regard to study objectives the questionnaire was developed in order to address the following areas:

- Establish the level of awareness/understanding of privacy (*Objective 1*).

- How is privacy policy developed? (*Objectives 2 and 3*)
- Technical issues regarding privacy – problems / capabilities (this is related to the lexica later on – therefore, technical capability / limitations is important) (*Objective 3*).
- Who has access to data? (*Objective 2*)
- Who updates / manages / deletes data? (*Objective 2*)
- Authorization. (*Objective 2*)
- Authentication. (*Objective 2*)
- Geographic location. (*Objectives 2 and 3*)
- Where system is distributed? (*Objectives 2 and 3*)
- Establish the level of interest in privacy. (*Objective 1*)
- Establish the extent of human and technology barriers to maximise the use of effective privacy policy between users. (*Objective 2*)
- Establish the level of satisfaction with the current way of sharing information and privacy measures. (*Objectives 1 and 2*)

In accordance to the aims and objectives of the study another objective of the questionnaire was to address the perceptions of privacy of the users of distributed systems, in light of this, the questions were developed in order to address the following issues :

- Establish the level of awareness/understanding of privacy. (*Objective 1*)
- Identify where perceived weaknesses in privacy. (*Objectives 1, 2 and 3*)
- The level of importance assigned to privacy. (*Objective 1*)

- What are the aspects of privacy? (*Objectives 2 and 3)*
- Which parts of a DS do users feel vulnerable? (*Objective 1*)
- Level of control. (*Objectives 1 and 2*)
- Who they feel should be allowed to access personal data? (*Objective 1*)
- Identify the most desired scenario of privacy measures. (*Objective 5*)

The findings of the questionnaire, in addition to the findings of the expert interview, contribute to an evaluation of the success or failure of current privacy policy strategies. This will show the weaknesses of current privacy policy strategy to justify the need for a new approach that considers the users' privacy expectations based on ultimately derived privacy perceptions. The followings areas are used as a basis for the questionnaire questions:

- User Empowerment/User Centric Enterprise
- User Empowerment/Transparent Enterprise
- User Space
- Business Space
- Effective Enterprise

The main purpose of the questionnaire was to facilitate the process of discovering and documenting the knowledge about privacy policy arrangements and IT associated information, and there were a number of questions related to the very nature of the enterprise departments' functions, as well as detailed questions about core services provided by the enterprise in relation to privacy.

Examples of questions:

Which device or technology do you use to access the distributed system? (Objective 1)

This question is aimed at establishing basic awareness about technology and its usage among participants.

Do you understand the enterprise privacy policy?

To reveal understanding and awareness of privacy policy **(Objective 1)**

What's your impression about the enterprise privacy policy?

This question is to reveal users perception and expectation of privacy when using the organization distributed system. **(Objective 1)**

Please list two events when you had to apply the privacy policy?

This one shows the user understanding, responsiveness and competence of the organization privacy policy. It also shows high degree of awareness of the privacy and privacy expectation in distributed system. **(Objective 1)**

In your opinion, what are the reasons behind the lack of enthusiasm towards the enterprise privacy policy?

This question is designed in order to identify users' perception shift between the enterprise's desire to assure client privacy and clients' expectations of privacy provision within the organization distributed system. **(Objective 1)**

3.4.2 Administrating the Questionnaire

The questionnaire was distributed directly to the respondents and a contact within each organisation that assisted with distribution and collection of the questionnaire. The questionnaires were self-administered; they must grade each statement using a descriptive method scale, with a five point response scale.

3.4.3 Questionnaire Sampling

The study adopted purposive sampling as it was necessary to include participants who were developers of DS, users of DS and the experts from the two private organisations namely; Al- Rajhi Bank and the Northern Cement Company, and the public body; the Technical and Vocational Training Corporation.

To achieve a suitable privacy policy, certain inclusion criteria were imposed. The participants all had to be qualified in their respective areas to ensure that the participants would understand the nature of the topic of the questionnaire and its use for improving privacy.

The Questionnaire Survey was conducted among users with a sample of n=100, 70 users and 30 developers.

3.4.4 Piloting the questionnaire

To test the validity of the questionnaire a small sample of six respondents was used. Once the questions were answered respondents were asked if there were any issues with the questionnaire in terms of clarity and comprehensiveness to improve the questionnaire and ensure validity. Defective forms were then disregarded and unclear or difficult terminologies were changed to make it more accessible simple to understand, in order to reduce ambiguity or comprehension issues.

3.4.5 Questionnaire analysis

Once the questionnaires were completed the total number responses for each item were tabulated. As for the qualitative analysis participant responses were coded to derive ideas and themes related to current privacy policy and privacy perception. Statistical analysis is applied on all the data using Excel software.

3.5 Post PPF Development Questionnaire

The PPF will be justified and developed based on the results of the aforementioned research instruments. Here the post PPF development questionnaire which is designed to determine the success of the framework from the perspective of the parties involved is presented. Users, developers and owners are questioned about the applicability and

suitability of the framework. This questionnaire form part of the overall validation for the framework.

3.6 Analysis Methods

Analysis of the results took place for the questionnaire and the post PPF questionnaire. The analysis was quantitative and represented the extent to which participants agreed or disagreed with statements regarding privacy and the PPF.

3.6.1 Quantitative Analysis

Statistics in common language use are a numerical way of describing a population, usually using a sample of that population. In the language of mathematics a parameter is used to describe a population, and a statistic is used to describe a sample. There are some statistics that are useful for describing results through measurement of a single variable, or for constructing and evaluating multi-item scales (variations on privacy policy between sectors, departments and technologies). These statistics include graphs, frequency distributions, measures of central tendency and reliability tests. Other statistics are used to describe the association between variables and in the controlling of other variables, for example enthusiasm for the enterprise privacy policy and understanding of the need for the policy, thereby enhancing the causal validity of our conclusions. This is especially done when conducting qualitative analysis. Cross-tabulation is one such technique that can measure the association and control other variables. All of these statistics are named

descriptive statistics of the method of this study, because they describe the relationship between and distribution of the variables. Statisticians also employ inferential statistics to quantify and estimate the level of confidence in generalisations from a sample.

3.7 Ethical Considerations

The nature of this research requires the participation of human respondents, specifically the senior managers of an enterprise, in particular for the employees of Al-Rajhi Bank plc, specific ethical issues were addressed which was necessary to ensure the privacy and safety of participants. The ethical issues that were considered important in the research included informed consent and confidentiality of the business and participant's. To secure the informed consent of the participants, they were informed them about the details of the study and its purpose, including its aim and rationale to them in accordance with the university standards and guide lines. By explaining these details, the participants to the study can understand their role in the research. Participant confidentiality is also ensured through not disclosing names or personal information in the study. Only important details that were relevant to answering the research questions were included. Participants were also reminded that they could pull out from the study at any time. It's also important to mention that the participants were not coerced to participate in the research; they participated on their own free will. This was achieved through the process of informed consent, something which is emphasized by ethical codes of practice that participants are aware of what they are consenting to and that they are not under duress (King and Horrocks, 2010).

3.8 Summary

This chapter presented the methodological approach of the present study and the associated methods that are employed. The theoretical foundation of the study reflected the idea behind the framework of the study which is based on considering both the objective and the subjective in relation to privacy, privacy perception and privacy in distributed systems. Thus the appropriate theory of ‘structuration’ was presented as the basis for the methodology. Based on this methodological approach, the research instruments that were designed to achieve the aims and objectives of the study were also presented.

Chapter 4

Privacy Policy Framework Design

Objectives

- Describes the need for a privacy based policy framework.
- Overview of privacy policy framework (PPF).
- Privacy expectations of users based on the disambiguation of privacy.
- Describes how the framework is based on the idea of a hybridisation of the technical considerations for privacy in distributed systems.
- Demonstrates the application of the PPF.

4.1 Introduction

This chapter presents the overall structure and function of the proposed Privacy Policy Framework (PPF). The framework requires a number of inputs which include the disambiguated meaning of privacy from users and developers of distributed systems, the literal (denotative) and metaphoric (connotative) meaning and the technical considerations for privacy in distributed systems. It is shown how the perceived meaning of privacy should be translated into privacy expectations before being hybridised with technical considerations for use in the development of privacy policy by the developers of distributed systems.

This chapter describes how substantial contributions were made to conception and design of privacy provision in DS through the development of a privacy policy framework (PPF). PPF considers the system design process from three different perspectives — Users, Developers and Infrastructure and guides the selection of techniques towards integrative Users, Developers, and Infrastructure engineering processes.

4.2 Overview of Privacy Policy Framework (PPF)

A description of the PPF as shown in figure 4.1 below is best described in terms of a process. Firstly the lexical and technical meanings of privacy are established and then disambiguated. This is achieved through the use of interviews and questionnaires. The disambiguated privacy then contains information about the technical considerations for privacy and perceptions of privacy which are then translated into privacy expectations.

At this stage the disambiguated technical considerations of privacy and disambiguated perceptions of privacy can then be hybridised to provide lexical – technical terms for privacy which are used as the input for the development of the privacy policy.

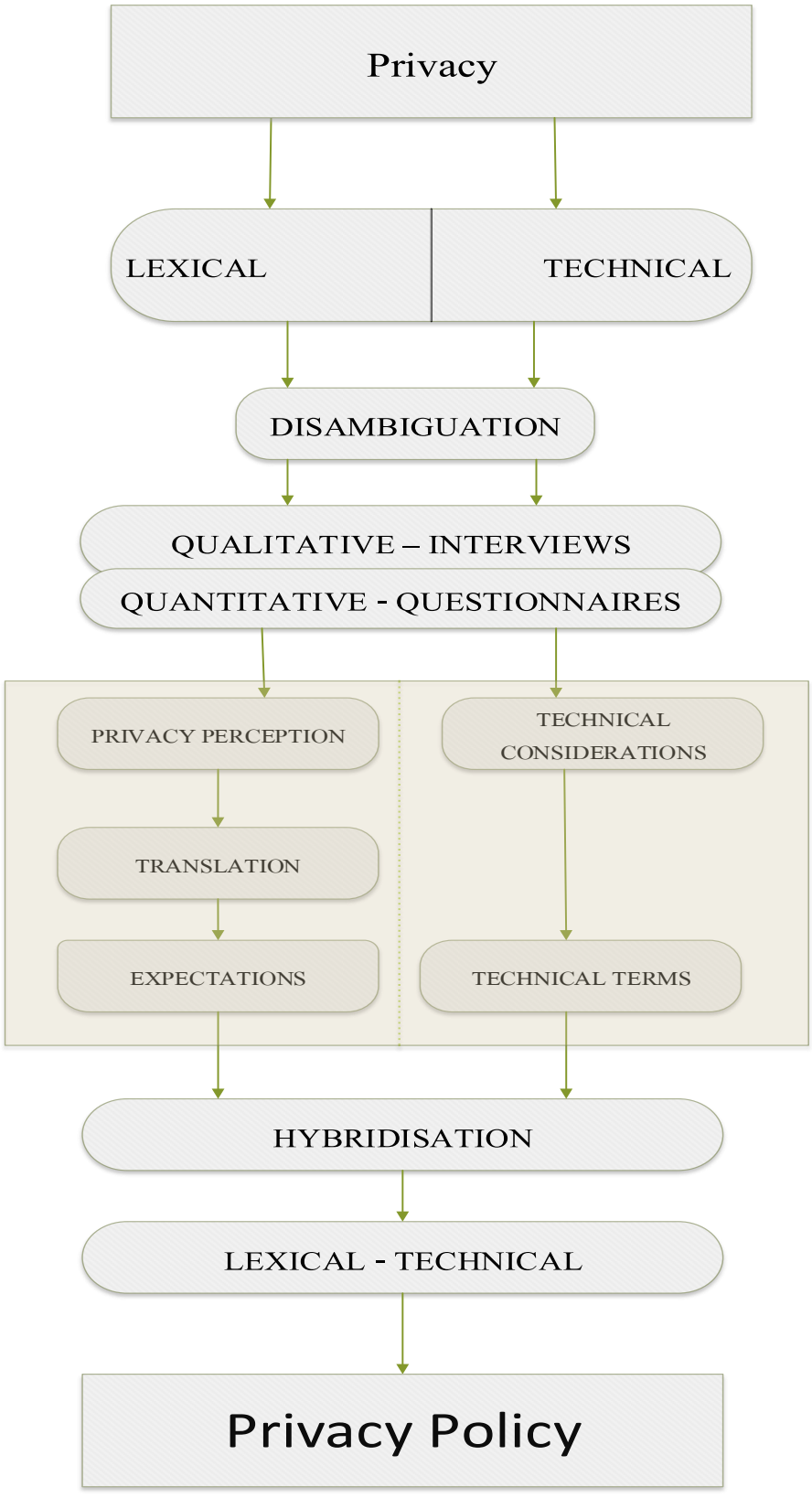


Figure 4.1: Privacy Policy Framework (PPF).

4.3 Background

Privacy in its cognitive manner cannot be achieved in a digital environment without consideration to its abstract and ambiguous nature. However, the problems of privacy are part of cognition and not distributed system environment only; therefore, current frameworks are less likely to achieve privacy provision through considering privacy perception of users. Hence our proposed privacy framework provides a better privacy approach by introducing a cognitive-technical concept into the framework design. For example, literal (denotative) definitions and metaphoric (connotative) associations are examined to explain privacy in relation to mental representation, concepts and perception. Moreover, because the framework also includes consideration of the technical, the method is tentatively grounded in the disciplines of lexicology, cognition and information technology. The analysis of this method is applied to the meanings of privacy including the definitions used by authors, IT developers and peoples in the research. Finally the study aims at proposing a pragmatic, semantic and conceptual framework for deriving perceptions of privacy. This semantic meaning of the term privacy establishes a new method of proceeding semantic and conceptual instances of privacy in relation to technology.

When privacy policies are written they are often focused on security, but privacy for the user is a far more complex idea. Despite engaging with privacy and security concerns during the early stages of design of distributed systems, a privacy policy framework. Without a better understanding of how to deal with concerns at an early stage, the design process risks disenfranchising stakeholders, and resulting systems that may not consider the privacy concerns of users.

Distributed Systems (DS) policies to protect privacy are similar, linear and less efficient in most DS. There exist a large number of cases of privacy breach in DS. Privacy breach is attributed in most cases to lack of capacity towards resolving issues of confidentiality expected by the user. Current methods lack understanding of the underlying reasons and principles central to privacy. Moreover, these attributed methods, methodology and processes are mainly consistent of DS architecture, lexicon and human, and system errors.

Thus, disambiguation of the meaning of privacy to users and developers plays a critical role in transforming privacy policy development from being static to being interactive and dynamic, towards delivering the user's privacy expectations. Privacy provision must incorporate user privacy expectation in an interactive manner; this expectation is derived from user privacy perception.

The present study proposes a new method that incorporates system developers and users to formulate, standardise and guide DS privacy terms.

The HPTM method enables parsing of grammar based descriptors into socio-perceptive, lexicon-morphing, conscious design of privacy-enabled systems. However, a range of dependencies exist surrounding systems design and perception of privacy, such as spatiotemporal, lexicon attenuation, connection and not premeditated processes (Thomas, et al, 2003).

The disambiguated meaning of privacy is based on a perception of privacy derived during the study. In order for this perception to be included in a privacy framework it is first necessary to translate these perceptions into expectations that can be easily considered and implemented into distributed systems.

The research problem this addresses is how socio-linguistics and socio-psychological tools can be integrated to support the design of a new privacy term development method. To develop this, a Hybrid-privacy term for specifying usable and secure privacy policies for distributed systems is presented where the privacy lexica-technical terms of polythematic hybrid privacy semantic methodology are specified.

The HPTM method considers the system design process from three different perspectives, users, developers and infrastructure, and guides the selection of techniques towards integrating the perceptions and expectations of users and developers in engineering processes.

4.4 Privacy Disambiguation

The analysis of construct definition based on information published in the literature, for example dictionaries are investigated under various conditions, for example semiotics. The new Hybrid-privacy method is Lexica-Technical approach that investigates these definitions of terms in relation to technology in distributed systems (DS).

The method is grounded in the disciplines of philology, cognition and information technology. The Lexica-Technical enquiry process is applied to the meanings of privacy starting with its original usage in the twenty first century and culminating with the definitions used by authors, IT developers and participants in the present study. Finally, the chapter aims at proposing a pragmatic, semantic and conceptual framework for measuring privacy. Finally, the chapter introduces an extra button on the keyboard to

indicate that any following activity is considered a private activity to establish new link between cognition and neuron-computation systems (Alhalafi, 2015).

In addition to the lexical side of understanding privacy through disambiguating the meaning of privacy perception, the framework also considers the technical issues that are relevant to the development of the privacy policy, these are issues that relate to the technical restrictions of the DS architecture and functions as well as the technical requirements of the organisation. These technical issues, i.e. the limitations of the technology and the organisational requirements are something that is already considered in the development of privacy policies; therefore, it is one of the contributions of the present study that it adds a lexical consideration of privacy to the technical considerations for policy development. This disambiguation is achieved through firstly, gaining the perceptions of privacy, and then secondly, translating the perceptions into privacy expectations. It is the disambiguated meanings of privacy that will be hybridised with the technical terms for privacy.

It is important for the framework to translate privacy perception into privacy expectation because the disambiguated meaning of privacy is based on privacy perception; unfortunately, it would be difficult for those who are involved in the development of distributed systems to take a disambiguated meaning of privacy into consideration during development of a privacy policy for DS. Therefore, as part of the framework of this study the perception of privacy is interpreted to derive privacy expectations which can then be used to develop the privacy policy and the associated integration of security in DS.

Thus the objectives of the disambiguation are to establish from the perspective of users the level of awareness and understanding of privacy, the level of interest in privacy, the barriers, both human and technological, to provision of privacy, the level of satisfaction of sharing information and privacy measures and finally, to identify the most desired scenario of privacy measures.

4.5 Hybrid Privacy Terms in DS

Hybrid privacy term refers to hybridisation between Distributed Systems Architecture and the user's perceptions of privacy. Specifically, the hybridisation is between the design of the DS in terms of architecture and technical considerations in terms of functional requirements and limitations and restrictions hybridised with the conceptual, i.e. the meaning of privacy.

In today's DS architecture, and dynamic constituent distributed system for users, this is guaranteed to cause major problems and user disappointment. However, a completely assimilated Hybrid-privacy term will motivate the smooth process of vertical and horizontal access across the user's perception and System design, resulting in a single holistic view of the user's expectation (Proc, 2014).

The HPTM method will extract perceptual terms from users and developers. In this study a new method HPTM (Hybrid Privacy Terms Method) is proposed that incorporates system developers, users and experts to formulate standardise and guide DS privacy provision. The relationship between DS developers and users, under the guiding principle

of conformity, is divided into user expectation, legal requirements and a distributed system risk strategy (Kenneally et al, 2010).

4.5.1 Primary Specification:

- Hybrid-privacy terms of privacy information
- Hybrid-privacy terms domain infrastructure capacity

4.5.2 Secondary Specification:

- Hybrid-privacy terms scale
- Hybrid-privacy terms domain weight communication perception

A simplified view is by distinguishing conceptualisation (knowledge), action in the world (practice), and text, diagrams, and computer programs (descriptions, commonly called "representations"), (Reips, 2006).

Therefore a descriptive method of research was used. The reasons behind selecting this method are to determine firstly, the factors of success or failure in relation to technology and secondly, to establish the factors of success or failure in relation to perception. The success or failure constitute one of the two dimensions that this paper seeks to define, the first dimension is the technology factor which includes what is permissible in terms of architectural design in terms of required functionality and limitations and the second

dimension is the human factor represented by privacy perception which includes what is permissible in term of user's privacy perceptions and expectations.

Dimension	Surveyed	Social-Psycho-devices method	DS Relationship
Technology Factor	Developer	Expert question	DS-to-Human-to DS
Human Factor	Users	Survey	Human-to-Human-to-DS

Table 4.1 Framework factors hybrid privacy system

In table 4.1 the possible distributed system dependencies are formulated under the DS Relationship column and are DS- to-Human-to-DS, which is an 'outwards' relationship and Human-to-Human-to-DS, which is, an 'inwards' relationship. Social-Psycho tool methods are divided into qualitative and quantitative outputs capturing dimensional factors from users and developers.

Therefore, the framework proposes to link two different processes that are running at the same time, the first process is the perception layer and the second layer is the design / infrastructure layer which is the responsibility of the system developer. The reason that this is necessary is because not only are privacy policies often standard, but because the

privacy policy of the developer could be completely different to the privacy perception of the user, these perceptions could even be opposed to each other.

4.6 Privacy Button

Including the perception of privacy and the associated expectations into a privacy policy has not only been beneficial in terms of considering privacy perception in the development of privacy policy, but, through the introduction of a privacy button has also allowed the development of privacy policies to be real-time and dynamic. This was achieved through the introduction of a button that allowed users to indicate activities that they feel are private when engaged with a distributed system. This extends the idea of considering privacy perception, as proposed by the PPF, to real time use of the system.

The framework is based on the idea that the perception of privacy is something that should be considered in the development of privacy policies, however, privacy perception is something that continuously changes perhaps from events in people's lives, education and the media and is unique to individuals. Moreover, it may not be changes in perception that is the issue, it cannot be expected that all perceptions of privacy can be derived from individuals through questionnaires and interviews, thus, there needs to be an additional way to derive privacy perception in real-time through use of the DS by users.

So while the framework is effective in taking privacy perceptions changing them into expectations and then combining these with technical considerations towards the development of privacy policy, the framework can only be applied to a particular set of

circumstances for a particular set of people. While the PPF is beneficial for organisations that want to develop a privacy policy according to the needs of their users, it does not offer a continuous assessment or reassessment of privacy perception on an ongoing basis. Therefore, there is a need to apply the principles of the PPF in a way that allows a continuous disambiguation of privacy in real time. This will contribute to a privacy policy that is dynamic and can react to changes in privacy perception in real time.

This is achieved in this study by the introduction of a privacy button on a keyboard that can be activated by the user when they are carrying out activities in the DS where they feel there should be privacy. Specifically, if the user feels that their next activity is private they can activate the button which provides a link between the cognitive and computation. The privacy button is therefore, a physical implementation of the PPF in real time. The aim of using a privacy button proposed in this study is to find a solution to the reoccurrence of privacy breach incidents in DS, formulate user / developer relations and hybrid privacy terminology, to reflect on both the user's expectations and the developer's design and interpretation of user requirements. In reference to the latter, the privacy button will inform the developer of the privacy policy about privacy perceptions and expectations as they arise. The privacy button extends the psychoanalysis that is an essential part of the PPF answering the need for qualitative information related to users' realisation of privacy in DS to a physical component or a physical application of the PPF principles.

Figure 4.2: Illustration user privacy input captured

The aim of carrying out a descriptive survey on users' perceptions of privacy is to verify the study's primary specifications which is to disambiguate the meaning of privacy which can be achieved an ongoing process with the introduction of a privacy button towards an up-to-date and relevant privacy policy (Alhalafi, 2015).

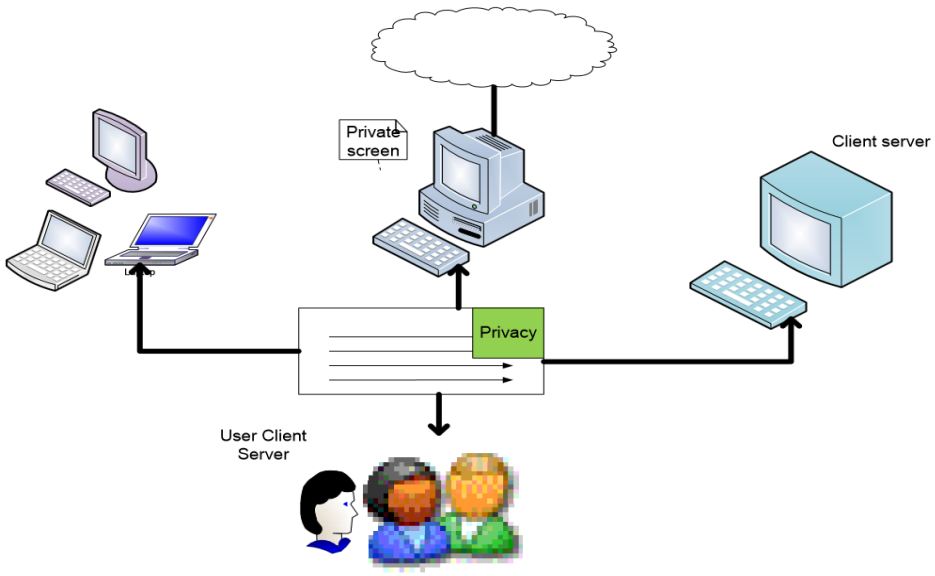


Figure 4.3: HPTM method application illustrations

The privacy button method offers a rapid and practical method for the development of privacy policies for distributed systems through informing about the individual nature of privacy perception.

4.7 Summary

For several reasons this study is relevant within security, access control and distributed systems. The first, and most important aspect of the PPF is that it focuses on contributing to the development of privacy policy in DS and therefore, has implications on the implementation of privacy provision strategies in distributed systems.

This chapter has shown how privacy issues, terms and concepts, in the light of a new approach, can introduce an innovative concept of privacy which includes perception and expectation. Moreover, real time consideration of the cognitive has been proposed, through the use of a privacy button, which allows the hybridisation of the Lexica-Technical of the PPF to be extended. Further, guidelines for privacy disambiguation have been defined by the PPF; a privacy based framework proposed to fill the gap between privacy perception and expectation and privacy implementation through a proposed privacy based HPTM method as part of the overall PPF.

In the following chapter there is a demonstration of the application of the framework in three organisations, this is achieved through questionnaires and interviews, the results of these are presented towards achieving privacy disambiguation.

Chapter 5

Application of Framework - Results and Analysis

Objectives

- Presents the results of the questionnaires and interviews.
- Present the associated results relate to the existing situation with privacy policies in their respective organisations.
- Provide information about the existing privacy frameworks.
- Demonstrates application of PPF based on results

5.1 Introduction

There have been a number of studies related to privacy perception and privacy evaluation strategies (Aichholzer, 2004; Bhatnagar, 2004; Chen et al, 2006; Heeks, 2006; Shahkooh and Abdollahi, 2007). Most of these studies have shed light on to what privacy perception and privacy evaluation strategies should be like or how they should be planned. Some other contributions sought to produce strategies aimed at better understanding of privacy as a concept. Each attempt tackled the complexity of privacy from a certain perspective, such as, divisible and non-divisible privacy perception semantic. This chapter presents how the framework is applied as a strategy for privacy perception elicitation which forms part of the overall disambiguation of privacy.

This chapter presents a demonstration of the practical application of the PPF through the use of questionnaires and interviews and shows how the PPF can be applied in terms of the Lexical – Technical hybridisation of terms. This is followed by the results of the questionnaires and interviews and the derived perceptions of privacy.

5.2 Lexical

As described in the PPF there needs to be a hybridisation of terms approach to the development of privacy policy. Here the practical application of the PPF is demonstrated for deriving the lexical meaning of privacy. Specifically, this involves two stages, firstly, the perception of privacy, and secondly, the translation of privacy perception into privacy expectations.

5.2.1 Privacy disambiguation – Perceptions

The measures for deriving privacy often include consideration of breaches of privacy. Therefore, the PPF is designed to reveal incidents of breaches of privacy from users and in light of this questions about breaches of privacy are included in the questionnaire. Thus a central aspect of the proposed framework is that it uses counts of privacy breaches.

In accordance with the PPF there is a need to derive the meaning or perception of privacy for the parties that are involved in the development, management and use of distributed systems. This is considered the part of the overall disambiguation process before privacy expectations are derived. Therefore, as part of demonstrating the application of the proposed PPF, this study conducted interviews and questionnaires with experts (senior management), developers and users of distributed systems in order to derive privacy perception, the findings of these interviews are presented in the following chapter.

5.2.2 From Perception – Expectation

The framework included the final stage of the disambiguation process which was to take the derived meanings of privacy and convert them into expectations. In order to apply this part of the framework it was necessary to derive the perception of privacy through the questionnaires and interviews and then translate those perceptions into expectations. It should be noted that this translation was done based purely on the logical expectations for the perception of privacy and the expectations that could be derived from the responses to the interviews and questionnaires.

To provide an example, there is a question that is related to the need for awareness of personal information disclosure. This question helps to understand the perception of privacy in terms of the fact that participants see it as a right that they know where their personal information is disclosed, and the associated expectation would be to disclose that information. The following table 5.1 provides some examples of derived perceptions of privacy and the associated expectations that are subsequently used in the development of the privacy policy.

Perception	Expectation
Privacy is about knowing where my information is distributed	User should be informed of where information is disclosed
Privacy is about control over private information	User provided with facility to control private information

Table 5.1: Derived perceptions to expectations

5.3 Technical

As described in chapter 4, the framework considers the definition of privacy in relation to technology and this will form the technical side of the Lexical –Technical hybridisation.

In accordance with the methodology and the proposed PPF it is necessary to understand the technical aspect of the DS and privacy policy, this will form the technical side of the Lexical-Technical terms. In applying the PPF in this study, as part of demonstrating the PPF, it was important to determine the technical considerations. This would include both the questionnaires and the semi-structured interviews which were employed to derive information about current technology used related to the provision of privacy. Specifically, as part of the PPF, information is needed about the DS architecture because it is important to know the limitations of the DS in terms of the type or level of privacy provision that it can provide. Moreover, it is necessary to understand the organisational requirements from the technology that have an influence on the privacy policy. This information will for the technical side of the hybridised terminology – Lexical – Technical. It is important to note that whatever perceptions and associated expectations are derived, they are bound by the technical / architectural consideration related to the DS. Therefore, as part of the demonstrated application of the PPF, this study conducts interviews and questionnaires with experts and developers respectively in order to derive information about technological limitations and organisational requirements of the technology.

5.4 Hybridisation of Lexical and Technical Terms

As shown in the chapter 4 the PPF uses a hybridisation of the lexical and technical terms for describing privacy which are used to specify the privacy policy. Thus the design of the distributed system is based on meaning derived from the users and developers of such systems and the technical considerations of the system itself which include its architecture and limitations. Therefore, the hybrid privacy terms refers to hybridisation between the system architecture and the derived perceptions of privacy.

The derivation of the perceptions of privacy has been described. For the derivation of the technical considerations such as system architecture there is a need to consult with the developers and the managers responsible for the distributed systems. In this study there is demonstration of the PPF through application described in this chapter and demonstrated in the following chapter (Include this idea in the introduction). Once all of the terms, both lexical and technical have been derived they are combined as lexical-technical terms, show in Chapter 6. In the present study this hybridisation of the lexical and technical terms is referred to as the HPTM (Hybrid Privacy Terms Methods) which has already been presented in chapter 4. The HPTM guides the selection of techniques towards integrating the perceptions and expectations of users and developers in engineering processes.

5.5 Practical Application of PPF

This section presents the results of the interviews with experts and questionnaires conducted with developers and users of distributed systems as a demonstration of the application of the PPF. Both survey instruments were designed to find out the current situation in the respective organisations as regard the privacy policy. This forms part of the justification of the study, in that it aims to identify where current privacy policy falls short of responding to the privacy concerns of users towards deriving privacy perceptions. This forms part of the disambiguation of the meaning of privacy which is part of the overall proposed framework.

5.6 Current Privacy Policy and Privacy in DS

Both interviews and questionnaires were employed to establish the current privacy policy at the three sample organisations. Specifically, the interviews and questionnaires were designed to investigate current issues related to privacy policy and the aforementioned technical considerations both in terms of architectural or system constraints and technologically related organisation requirements placed on the DS.

5.6.1 Results of Experts' Interviews

The research used interviews to ascertain the current privacy policy situation that exist in the three organisations represented by their respective senior managers. The interview

was based on six areas designed to ascertain the current privacy policies. The results are presented according to each of these areas.

5.6.1.1 The ability of the available privacy policies to offer the best service to the users

All the ten of the interviewed senior managers stated that the development of their privacy policies was tailored to provide high-level privacy to the users. They agreed that their systems met all the requirements of an ideal privacy policy.

5.6.1.2 User to user (U2U) services provided by the enterprise in respect to privacy

The interviews identified four U2U services provided by the enterprises and they include monitoring, secure analysis services, backup and restoring and installing analysis services.

5.6.1.3 How the information systems support the U2U services

The participants indicated that their information systems supported various U2U services through the provision of account information, notifications and message conservation. Additionally, the information system supported the U2U services through system training, smartphone apps, client checklists and configurations and customer education. However, the support varied depending on the organisation.

5.6.1.4 Privacy issues in the U2U services and evaluation of the privacy policy.

The privacy issues of the U2U services identified in the interviews included the limited

customisation of the websites as well as the impossibility of bug-tracking. The participants indicated that these two challenges were a result use of JavaScript frameworks. As a result, the privacy is compromised by the limited functionality and the lack of customised repositories.

5.6.1.5 Provision of a privacy policy for the enterprise.

The interviewed experts indicated that the use of in-house developed U2U services was more prevalent than the outsourced provisions. Eight of the ten participants indicated that their enterprises used in-house developed U2U services.

5.6.1.6 Accessibility of the privacy policies to the users with special needs.

The interview established that only four of the ten experts said their privacy policies were accessible to persons with disabilities. However, the remaining six participants indicated that people who are sight impaired could not access the privacy policy terms of their enterprises. However, where it was mentioned by the experts where disability was addressed it was audio files for the sight impaired.

5.6.1.7 Technological constraints of the DS that are relevant to privacy provision

One of the issues that arose was the fact that although distributed systems are pervasive the databases that contain much of the private information can be found in a limited number of locations and have a specific owner; this was due to a decentralised system of control. This was said by the experts not only to be technological constraint on the formation of privacy policy, but a weakness in privacy provision.

5.6.1.8 Organisational requirements of DS that impact on privacy provision

According to the responses one of the main organisational requirements is related to the fact that information has to be made available to different parts of the organisation and different individuals also require access to personal data. However, there was an emphasis that there were clear guidelines for the handling of this data. Moreover, there was the idea that some of the systems within the distributed system would not work if they did not hold private data.

5.6.2 Results of Questionnaires – users and developers

A questionnaire was distributed to users and developers to help establish the personal understanding of the current privacy policy. In addition to the personal understanding the questionnaire also sought to establish the awareness of the privacy policy as well as the privacy policy expectations of the distributed system that need to be met in order to protect system users, as well as the causes of the lack of enthusiasm for the use of the privacy policy in the distributed systems. The results of the questionnaire are organised according to the areas that were investigated.

The questionnaire also tried to establish the privacy perception of the users, developers and experts in relation to the need to create secure distributed systems.

5.6.2.1 Awareness of the function of the enterprise privacy policy

In order to check the participants understanding of the organisational privacy policy a question to determine the personal awareness of the function of the enterprise privacy policy was included in the questionnaire. The participants gave a strong positive response, indicating a high level of awareness of the function of the enterprise privacy policy. In the questionnaire survey, 94 of the respondents said that they were aware of the function of the enterprise privacy policy (see figure 5.1).

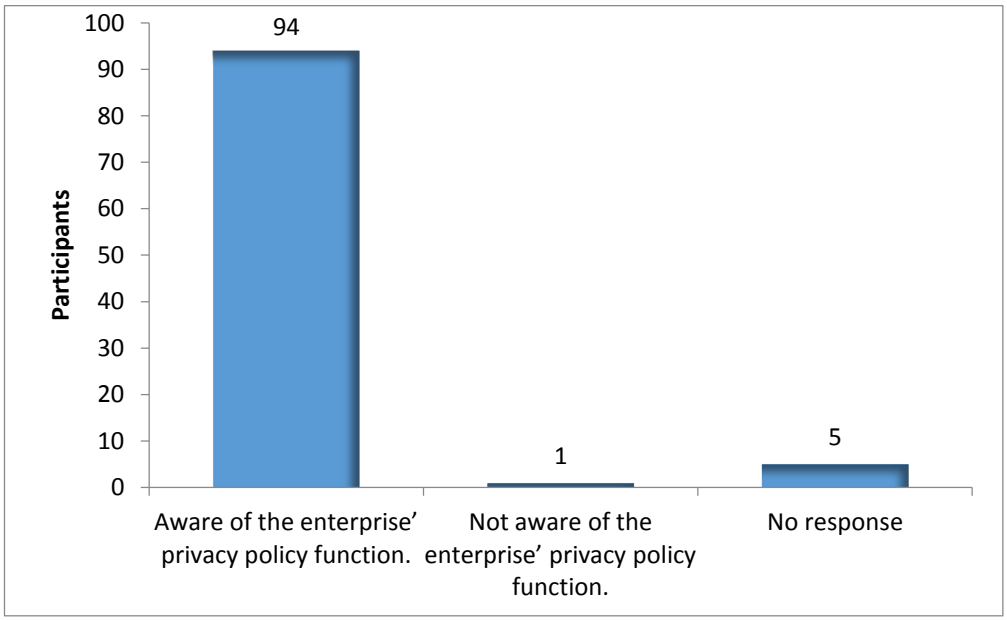


Figure 5.1: Awareness of the function of the enterprise privacy policy – users and developers

5.6.2.2 Opinions about the enterprise privacy policy

For the survey to establish how different participants regard the enterprise privacy policy, the questionnaire sought the opinions of each user and developer about the enterprise privacy policy. Generally, the participants had various opinions, all stressing not only the importance of a privacy policy but also some of its inadequacies in ensuring the security of privacy in the organisation. Both the users and the developers were more inclined to the idea that the enterprise privacy policy seeks to protect the system users from misuse, alteration or loss of information under the enterprise' systems and computer networks. However, a significant number of participants felt that an enterprise privacy policy does not guarantee the protection of all privacy needs and 36 of the participants agreed with the idea of using better approaches to ensuring the security of their information. The opinions generated by the question are be classified into four categories as expressed in the following table (see table 5.2).

Table 5.2: Opinions about the enterprise privacy policy.

Respondents	Opinion that the enterprise privacy policy is enough in ensuring the information security	Opinion that the enterprise privacy policy is not enough in ensuring the information security	Opinion that the enterprise privacy can be better accomplished through other approaches	Opinion that the enterprise privacy cannot be better accomplished through any other approach	No opinion about the enterprise privacy policy
Number of users	11	26	28	5	0
Number of developers	1	15	8	6	0

5.6.2.3 Events where the privacy policy has offered protection

The research also sought to establish where the participants perceived events where privacy policy was useful in protecting against privacy infringement. The question aimed at generating a list of incidents experienced by participants that were handled through the privacy policy. The aim of the question was to show the participants' understanding of responsiveness and ability of the policy as well as understanding of the privacy policy itself.

The list was short and limited to a few privacy concerns. A large majority of the participants said that they were afforded protection by the privacy policy against infringement of personal information and the exposure of usernames and passwords at 81 and 89 respondents respectively. A quarter of the respondents mentioned that the privacy policy protected their medical information, in Saudi Arabia it is a requirement that all employees undergo a medical examination as a condition of employment and the records are kept with the employer. The frequency of these events as expressed by the respondents is outlined in the table below.

Table 5.3: Events where the privacy policy has offered protection

Event where privacy policy offered protection to the respondent	Number of the respondents who perceived protection from privacy infringement from privacy policy
Protection from the disclosure of personal information	81
Protection from the disclosure of employment	13
Protection from the disclosure of medical history information	25
Protection from the disclosure of usernames and passwords	89

5.6.2.4 Reasons for the lack of enthusiasm towards the enterprise privacy policy

The questionnaire also sought to establish the reasons for the lack of enthusiasm for the privacy policy. The responses will help to understand why the participants are not

enthusiastic to use the privacy policy in their respective organisations for information security. The participants cited the method of obtaining consent, that the privacy policy is limited to online, and finally, third-party policies.

The users observed that the most systems assume that a consent form is signed simply by clicking a mouse. Users were also concerned about the fact that the privacy policy is mostly limited to online activities undertaken by the user. Moreover, the users showed unwillingness in reading the terms the privacy policies of third-party systems. The developers expressed similar views to the users; however, they added the use of log files as a fourth reason for the lack of enthusiasm for the application of the privacy policy. In their view, the logged information does not provide personally identifiable information to help support the organisation's privacy policy.

5.6.2.5 Areas of concern of privacy violation at work

The questionnaire also sought to establish the areas that were of concern to participants in terms of privacy violation. The participants provided varied responses that can be classified into five types of potential incident they were concerned about. These potential incidents included telephone monitoring, computer monitoring, mobile devices monitoring, email monitoring, and social media monitoring. Although there was a difference in the frequency of these potential violations, every participant gave at least two incidents from within this classification.

Table 5.4: Areas of concern for potential privacy violation

Class of the potential incident of privacy violation at work	Number of concern by participant
Telephone monitoring	43
Computer monitoring	48
Mobile devices monitoring	55
Email monitoring	35
Social media monitoring	62

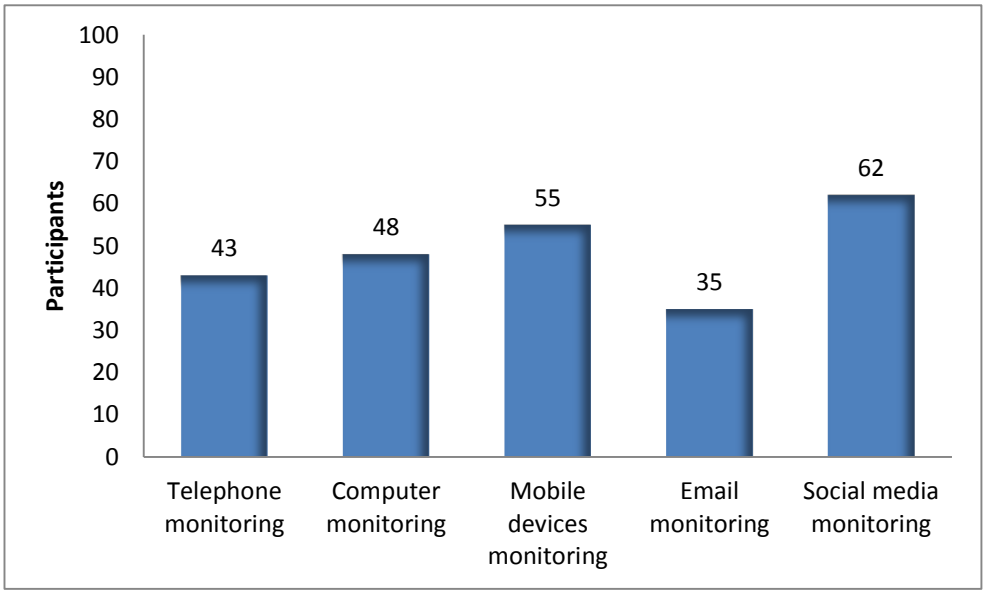


Figure 5.2: Areas of concern for potential privacy violation

5.6.2.6 Effectiveness of the privacy policy in making participants feel secure

The privacy policy of an organisation's distributed system should make system users feel secure. A measure of the effectiveness of a privacy policy is the extent to which it makes participants feel secure. The questionnaire sought to measure participants' feelings by using level of agreement on a Likert scale. Overall a large number of the participants, 48, either disagreed and strongly disagreed with the idea that the privacy policy made them feel secure (see table 5.5). However, a large proportion of the respondents, 37, were undecided about the issue.

Table 5.5: Effectiveness of the privacy policy in making participants feel secure

Privacy policy makes you feel secure	**Number**
Strongly agreed	2
Agreed	13
Undecided	37
Disagreed	39
Strongly disagreed	9

5.6.2.7 Suitability of the privacy policy for personal or organisational needs

The personal or organisational expectations in relation to the privacy policy determine how well such policies are suitable for the application. The users and developers of the systems have first-hand experience of the shortcomings of privacy policies. As a result, they are in a position to provide information about the suitability of the privacy policy in terms of personal and organisational needs. The questionnaire sought to establish the level of the respondent's agreement with the view that the privacy policy suited their personal and organisational needs on a Likert scale of five responses. The results that 48 of the respondents either disagreed or strongly disagreed with the statement that privacy policy suited personal or organisational privacy needs and only 17 agreed with the statement, it is interesting to note that a significant 31 respondents were undecided (see Table 5.6).

Table 5.6: Agreement with idea that privacy policy suits personal and organisational needs

Privacy policy suited the personal or organisation's needs	**Number**
Strongly agreed	4
Agreed	17
Undecided	31
Disagreed	38
Strongly disagreed	10

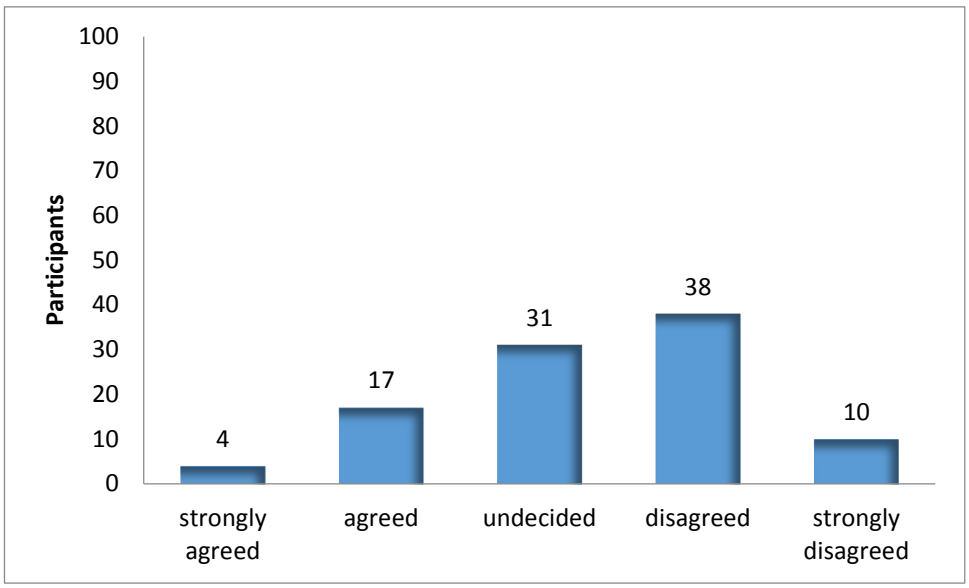


Figure 5.3: Agreement with idea that privacy policy suits personal and organisational needs

5.6.2.8 Consultation with the user during the development of the privacy policy

The relevance of the privacy policy of an enterprise depends on the views of the users during the development phase. The level of the user's consultation during the development phase determines the awareness of their needs among the developers. If a privacy policy is developed with the absence of the consultation of the end user, it becomes irrelevant in meeting their privacy needs. On the other hand, if the privacy policy is developed in consultation with users the needs of the end user will be met. In this survey, the relevance of the privacy policies was determined by seeking to establish the level of consultation with the users in relation to their development. Because the consultation relationship involves two parties; at the one end the user and at the other end the developer, the results are presented for users and developers separately.

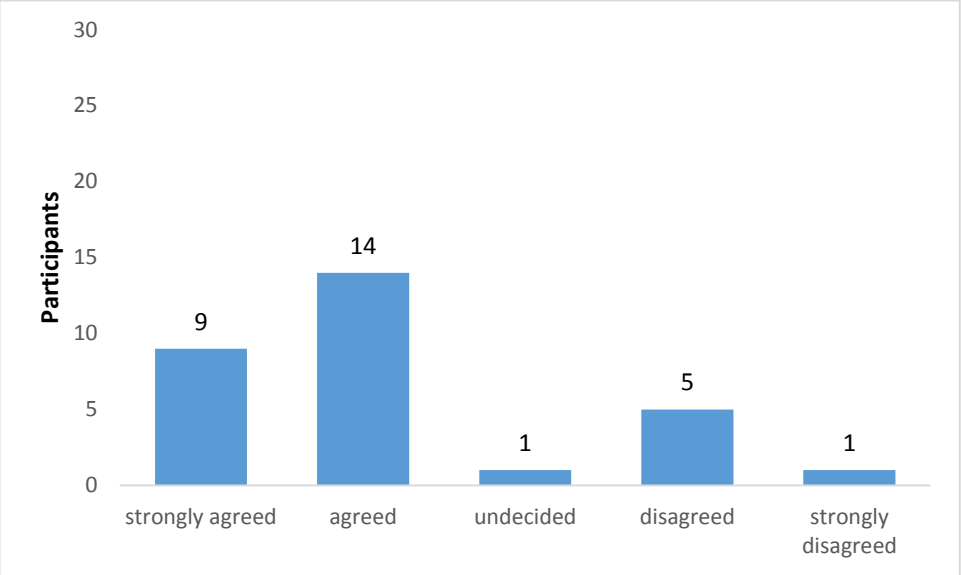
The results showed a clear contrast between the opinions of the users and developers. The users were very much in disagreement with the idea that they are consulted during the development of the privacy policy, a total of 49 respondents were in disagreement of which 20 strongly disagreed with the idea compared to 18 respondents who were in agreement (See Table 5.7).

Users are consulted during the development of the privacy policy	**Number of responses (Users)**
Strongly agreed	3
Agreed	15
Undecided	3
Disagreed	29
Strongly disagreed	20

Table 5.7: Agreement that users are consulted during privacy policy development (Users)

During the framework development of the privacy policy, the developers use the views of the users to determine the needs and expectations that need to be considered in order to tailor a relevant privacy policy. There was a sharp contrast in the results for the developers who strongly agreed with the statement. The results showed that a majority of the developers, 23, agreed with the idea that users are consulted during the development of the privacy policy of which 9 strongly agreed with this idea (see Figure 5.4).

Figure 5.4: Consultation of the user during the development of the privacy policy (Developers).



5.6.2.9 Methods of consultation about the personal privacy needs

The quality of the privacy policy also depends on the method of consultation with the users about their needs. Some methods produce biases that ultimately result in unsuitable products. The survey sought to ascertain the credibility of the level of consultation by establishing the techniques employed. The participants provided seven techniques that were used in their consultation when the privacy policy was being developed. The methods of consultation applied in the process included workshops and discussion groups, open days, web-based forums, polls and interviews and surveys which were the most popular (see Table 5.9). Some of the respondents indicated more than one technique.

Technique of consultation used in the development of the privacy policy	Number
Polls	23
Interviews	25
Internet-based forums	20
Open days	33
Workshops and discussion groups	29
Surveys	42

Table 5.8: Methods of consultation about the personal privacy needs

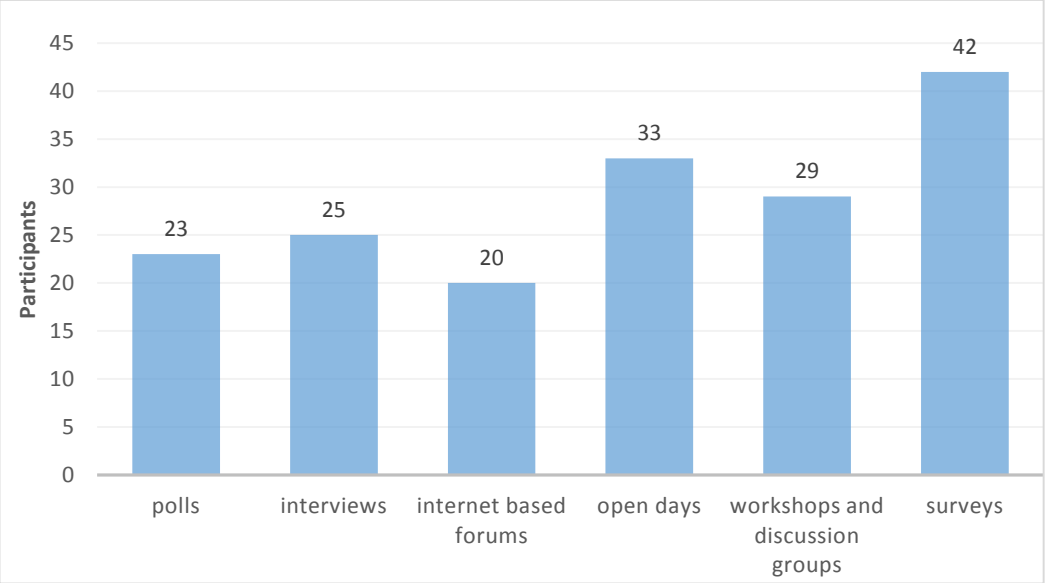


Figure 5.5: Methods of consultation about the personal privacy needs.

5.6.2.10 Developers' view of the privacy policy development

The developers view on the development of the privacy policy is reported here because they are the group responsible for such development. The quality and the relevance of the privacy policy is dependent on the how it is developed by the developers. A privacy policy development process that observes best practices is likely to be aligned with the needs of the users of the distributed systems. The questionnaire survey sought to establish what the developers considered during privacy policy development. The developers said they used a series of steps and all of them pointed out that their privacy policy was written in a language that was easy to comprehend. They also mentioned that their privacy policy indicated information about the enterprise affiliations. Moreover, the developers said that their privacy policies were compliant with the legal requirements of privacy and information and that the privacy policy allowed the readers to correct, verify, remove or change their personal registration information. They also indicated that the policies would be subject to future updates.

5.6.2.11 Technological constraints that may influence privacy policy

A number of the developers said that the design of the system or the system architecture was something that they has to consider when implementing a privacy policy, moreover, they said that the design of the DS often places limitations on what they do in terms of privacy provision. It is important to note that they also said that this cannot be resolved unless the system architecture is changed which is unlikely because the architecture is required for system functionality.

5.6.2.12 Organisational requirements of system that impact privacy provision

The developers said in relation to this question because the systems are distributed and designed to service many people in the organisation it is difficult to consider privacy provision, and that the nature of the system being widely distributed means that it is difficult to consider the privacy of all the different parties with the organisation.

5.7 Privacy Perception

Privacy and security needs in distributed systems are only achievable if the all the aspects of privacy are incorporated in the development for the privacy policy, this includes the disambiguated meaning of privacy as proposed by the framework of this study. In this section of the results the various aspects of privacy perception as indicated by the perceptions of the participants are presented. The questionnaire employed six statements to help establish the privacy perceptions of the participants.

5.7.1 The need for the awareness of personal information disclosure

The questionnaire sought to establish the level of need to be aware of personal information disclosure for all participants and determine their perceptions. To achieve this, a statement was presented to the respondents to determine their perception. The perceptions about the need for personal awareness of when and where personal information was disclosed were determined on a five-point Likert scale of agreement. The results of the questionnaire showed a majority of the participants, 18, agreed with the idea

that there was need to be aware of when and where personal information is disclosed (see Table 5.9). In contrast there was a very low level of disagreement with this statement with 14 respondents disagreeing and one strongly disagreeing. This clearly indicates that people are concerned about when and where their personal information is disclosed.

There is a need to be aware of when / where personal information is disclosed	**Number**
Strongly agreed	47
Agreed	18
Undecided	20
Disagreed	14
Strongly disagreed	1

Table 5.9: The need for the awareness of personal information disclosure

5.7.2 The need for information about personal information disclosure

Systems' users have varied perceptions about being informed when their personal information is shared. Some people regard such information as medical history, financial records, marital status, contacts and age, amongst others as very confidential. In such cases, a person may need to have the information about events of where and when such information is shared with any party. For this questionnaire aimed to establish the preference of the respondents to be informed of the disclosure of their personal information, a statement was presented for this purpose. A majority of the participants,

47, agreed with the statement that they need to be informed of their personal information disclosure and 15 of the respondents strongly agreed (Table 5.10).

The need to be informed about the disclosure of personal information	Number
Strongly agreed	15
Agreed	47
Undecided	20
Disagreed	10
Strongly disagreed	8

Table 5.10: The need for information about personal information disclosure

5.7.3 The need for the ability to control private information disclosure

Some people need to control the disclosure of their private information, and the ability to do so can positively impact one's perception of privacy at work. The ability to control the level of disclosure of personal information places system users in a position to control to whom, when and where their private information is disclosed. The questionnaire survey presented a statement to establish the level of agreement with the idea that they should have the ability to control the disclosure of their private information. A significant majority of the participants, 47, said that they agreed with the idea that they should have the ability to control private information disclosure and 19 strongly agreed (see Table

5.11). This was in sharp contrast to those who disagreed with this statement at only 8 respondents, with only 3 strongly disagreeing with the idea.

The Respondent's Need for The ability to Control Private Information Disclosure.	Number Of Respondents
Strongly agreed	19
Agreed	47
Undecided	23
Disagreed	8
Strongly disagreed	3

Table 5.11: The need for the ability to control private information disclosure

5.7.4 The need for a mechanism to offer full control of private information disclosure

The need to control private information disclosure requires the use of a mechanism. When a system' user has a full control of the disclosure of their private information through the use of such mechanism the privacy level increases because no one would access the information without the direct and full approval of the owner. This study sought to establish the number of individuals who would agree with the establishment of a mechanism to offer full control of their private information. The level of agreement was measured on a five-point Likert scale of agreement. A significant majority, 48 of the

respondents, agreed with the idea of a mechanism to control information disclosure with 12 respondents strongly agreeing with this idea, however, it is interesting to note that 30 respondents were unsure about this issue and the level of disagreement was low with only 8 respondents (see Table 5.12).

There is a need for a mechanism to offer full control of private information disclosure	**Number**
Strongly agreed	12
Agreed	48
Undecided	30
Disagreed	8
Strongly disagreed	2

Table 5.12: Need for a mechanism to offer full control of private information disclosure

5.7.5 Logging of activity in DS

Most systems include a history log for personal information. Some users feel uncomfortable with the idea that their activity is logged and feel that it is an invasion of their privacy. The development of a privacy system in a distributed system is partially dependent on the how comfortable the users are towards the logging of their personal activities in the systems. The questionnaire sought to establish the levels of comfort among users about user activity being logged. The majority of the respondents, 40, were clearly comfortable with the idea that their activity in the distributed systems is logged

and 16 strongly agreed with this idea. Only 28 respondents were uncomfortable with the idea (see Table 5.13). The logging of activity is something that most people should be aware of and such information is used to protect users in terms of privacy and security.

Comfortable with logging of personal activities	**Number**
Strongly agreed	16
Agreed	40
Undecided	10
Disagreed	28
Strongly disagreed	6

Table 5.13: Preferences about the logging of personal information

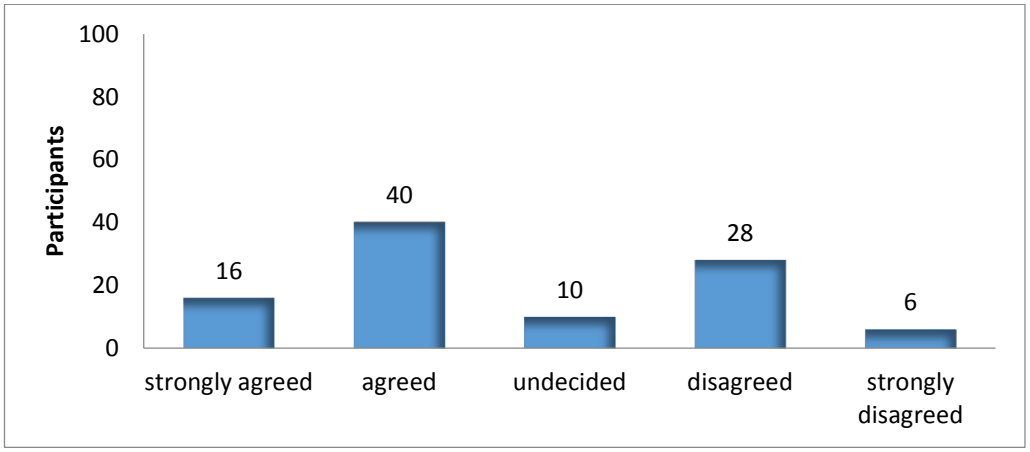


Figure 5.6: A graph showing references to logging personal information

5.7.6 Ability to adjust involvement in privacy in order to reduce the effort needed to manage personal privacy

Personal privacy in the distributed systems requires the involvement of both the users and the entire enterprise to ensure the maximum benefits. When the user has the ability to adjust his or her involvement in privacy they are able to control, to a certain extent, where and who can access their personal information as well as the time it is accessed. The questionnaire sought to establish whether or not participants thought it important to have the ability to adjust their involvement in privacy in order to reduce the effort needed to manage their privacy. The findings indicated that half of the respondents agreed with this idea and 20 respondents disagreed (see Table 5.14).

Ability to adjust involvement in privacy in order to reduce the effort needed to manage personal privacy	**Number**
Strongly agreed	12
Agreed	38
Undecided	20
Disagreed	20
Strongly disagreed	10

Table 5.14: The preferences about the ability to adjust involvement in privacy

5.8 Lexical – Technical Terms for Privacy Policy

As mentioned in the above the framework brings together both the lexical and the technical. In the above interviews and questionnaires were conducted in order to derive technical issues. These technical considerations based on purely technical considerations that have a bearing on privacy provision and organisational requirements related to technology of the DS that place restriction on privacy provision. This is based on the premise that it is not enough to consider the privacy expectations of the users, there needs to be consideration of the technical as well. As mentioned in the above the framework will create a hybridisation between these derived technical considerations as terms and the lexical terms. Here a demonstration of this hybridisation is provided.

Table 5.15: Lexical – Technical Terms for Privacy Policy

Derived privacy terms – Perception (lexical)	Derived privacy terms – Expectations (lexical)	Derived privacy terms - Technical
Control	Ability to control	Control in hands of database owner
Informed	Mechanism to be informed of private information disclosure	Personally identifiable information not always available
Adjustment	Ability to adjust privacy levels	System requirements for use of private data Control of private data with database owners
Accessible	Ability to access private information held on DS	Personally identifiable information not always available

5.9 Summary

In summary, this chapter presented the findings of the interview and questionnaire and provided the results according to the understanding of the current situation of privacy in the participants' respective organisations and the perception of privacy. Both elements form a part of the proposed privacy framework of the study, the current situation contributes to the technical side of the framework and the perception contributes to the lexical side.

The results clearly showed a high level of concern about privacy among participants, although participants were aware of the function and importance of their organisation's privacy policy for distributed systems they did not express much confidence in these privacy policies, felt that they were not sufficient in terms of keeping users secure and were not suitable for personal and organisational privacy needs. Moreover, users were not consulted in the development of privacy policies and generally lacked enthusiasm towards them. In contrast, the experts expressed much confidence in the privacy policies to meet the needs of the users.

The results also revealed ideas about privacy perception. There was a strong agreement that people should be aware of where there private information is disclosed and to whom, moreover, privacy is something that should be controlled by the user of distributed systems and there should be the ability to adjust the level of privacy to suit individual needs. The following chapters presents a discussion of the results and their implication in this study.

This chapter has presented the application of the framework to disambiguate the meaning of privacy through deriving privacy perception and privacy expectation and derive the technological considerations associated with distributed systems and privacy. This was achieved through interviews and questionnaires. It was demonstrated how the lexical and the technical could be hybridised to inform the development of privacy policy in distributed systems.

Chapter 6

Discussion and Evaluation

Objectives

- Discussion of the result.
- Provide the result of the developed privacy framework.
- Discuss the implications of the results.
- Provide the evaluation for a new privacy policy framework.

6.1 Introduction

As the complexity and the distribution of the computer systems and networks increase new considerations of the user privacy are developing. The number of privacy issues is complicated by the overdependence of the privacy policies on the technical grounds of the computer systems, further drifting the aims of such policies from the needs of users. Most of the privacy policies also fail to consider the perceptions of the end users with regard to what they feel about privacy. New methods of addressing such dilemmas of privacy need to be based on the user's understanding as well as the expectations of privacy in distributed systems. This study proposed a framework that would take the technical considerations together with consideration of the privacy perception of users in the development of privacy policy frameworks. Understanding privacy perception was part of the overall privacy disambiguation which included understanding the meaning or perception of privacy from users and then translating those perceptions into expectations which could then be used in privacy policy development. Thus the study contributed to the understanding of organisations' privacy policies and associated technical considerations (which are objective considerations) as well as the users' privacy needs and perceptions through disambiguation (which are subjective considerations), which can be combined using the structuration theory approach towards the development of a better privacy policy. Through a better understanding of privacy disambiguation, enterprises could perhaps improve the privacy policies for their distributed systems. When a better distinction of the existing privacy policies and the privacy perception is drawn, it would be easier to establish or justify the possibility of a privacy policy-based framework to achieve the organisation's privacy. Developers, owners and users of distributed systems

have various subjective perceptions of privacy, and this affects their attitudes towards the organisation's views towards privacy. The subjective perceptions of the developers, owners, and users, together with the other factors i.e., affect the concept of the effective organisation's privacy policy.

The chapter also aims is to presents and discuss the PPF framework design. The PPF framework design attempts to provide for privacy provision by both, developers and users, the perception of privacy among users, experts and developers, and the transformation of privacy semantics in information technology. The chapter contributes to the literature by eliciting a number of important questions out and about the semantic versus design and perception of privacy such as; what defines privacy? What is privacy provision? What information aid business managers and software developers in their assessment of perception of privacy among users? And finally, how do users and developers use this information in developing their perception of privacy? Thus the study aimed to resolve two difficult issues: one the definition of perception of privacy and the other related to privacy provision.

This study claims that the PPF framework integrates existing techniques and tools towards the design of a reusable privacy framework (Dawes, 2008). In particular, the PPF framework makes three significant solutions towards the stated research problem. First, a concept for dealing with interpretation, perception and cognition design issues on privacy, upon which the PPF framework is founded; this concept provides and informs changes to distributed system requirements and specification techniques for improved interoperability in the design process. Second, several characteristics of methods needed to specify and disambiguate privacy are introduced; a set of criterion, constructors and

guiding principles are used to illustrate how these characteristics can be embodied. Third, how the results, which provide privacy perception, of applying the PPF framework can be used to improve the design of existing user-centred intended techniques for privacy provision design is described.

In summary, the research is validated by applying the privacy framework to three case studies where the privacy framework is used to specify privacy requirements for a privacy provision model used by Al Rajhi Bank, the Northern Cement Company and the Technical and Vocational Training Corporation.

6.2 Findings - Interviews

This research derived its findings from interviews and a questionnaire survey. With regard to the interviews, ten senior managers were interviewed to establish and ascertain the organisations' privacy policy strategies for their distributed systems. All the ten senior managers observed that the privacy policies of their organisations were tailored to offer the best levels of privacy to the users. The developments of the privacy policies have traditionally been based on the existing threats to privacy as well as the legal provisions about privacy. In the light of these considerations, it is possible to develop a perfect privacy policy but in practice it might present various deficiencies because of the numerous variables associated with the almost infinite possibilities of user's needs. The interviews also established that the firms represented by the ten senior managers offered such U2U services as a backup and restoring, secure analysis services, monitoring and installing analysis services. When used appropriately, these U2U services can help the

users of the distributed systems to access various system utilities without fear of privacy infringements. The interview participants also revealed that their information systems supported those U2U services through the provision of the account information, system training, notifications, message conservation, smartphone apps and customer education, amongst others. The U2U services connect people through various disintermediation practices. The privacy concerns related to the U2U services revolve around disclosure of such aspects of information as health history, financial records, and contacts, amongst others. Loss or misappropriation of the aspects of the U2U services constitute serious privacy infringements, and the impacts span not only the workforce but also the entire organisation. The participants also recognised limited customisation of websites and impossibility of bug-tracking as the major issues limiting the privacy of the U2U services (Tanenbaum & Steen, 2002). The lack of the ultimate customisation of distributed systems contributes to the privacy challenges because of redundancy. The interview also established that the organisations provided the privacy policy in-house, an aspect that creates the ability to develop custom privacy policies. However, this aspect does not solve all the privacy issues related to their distributed systems. The research interview also established that people with disabilities had limited access to the privacy policy, and it can be attributed to the technological limitations of developing systems of providing these policies to people with multiple disabilities like deafness and blindness.

However, the interview used qualitative methods of data collection, and it suffers such limitations as biases of the researcher. However, the interviewees' response to the interview questions is subject to the influence of the interviewers' presence and their response ultimately leads to the wrong interpretations.

6.3 Findings – Questionnaire

In the results it was shown that there was very little confidence that a user's current privacy policy would make them feel secure. The way that a user would judge this would be based on their privacy perception, therefore, this is a clear justification for the need to include this perception in the development of privacy policy, and without it the policy is simply based on ideas of security. Thus if a privacy should make a user feel secure it has to be based on expectations.

The survey established a high level of awareness of the function of the enterprise privacy policy. However, there were few who had the opinion that the policies offered enough security to the information. Their opinion that their enterprises do not offer enough security to information was echoed by the findings and that they did enjoy protection from privacy infringement of their personal information, employment information, medical history, and user names and passwords, respectively. The high numbers of various incidents of privacy violation at work as evidenced by infringements upon telephone monitoring, computer monitoring, mobile devices monitoring, email monitoring and social media monitoring shows that the enterprise privacy policy is deficient in ensuring the privacy of the users of the distributed systems. These findings expose the inadequacy of the privacy policy-based framework in ensuring the privacy in organisations. Achieving privacy for the users of the distributed systems is a difficult task regardless of the existing privacy framework because of the use of the internet. Faults of the network security systems, regardless of their magnitudes, expose the users to information theft, spamming as well as virus threats that can be used to tap such types of

personal information as credit card numbers, residence, and other personal information by individuals who are remotely located on the globe (Xiao & Pan, 2007).

The surveyed participants also indicated a general disagreement with the ability of the privacy policy in making one feel secure. Furthermore, nearly half of the participants disagreed that the privacy policies of their enterprises were suitable for application whereas only minority of the participants agreed that policies were suitable. These results complemented a large number of the participants who disagreed that their privacy policies helped them feel secure. With regard to the ability of the privacy policy framework for achieving organisation's privacy, the high proportion of the incidents of privacy violation, low trust on the privacy policy and the inability of the privacy policy in making the distributed systems' feel secure is indicative of the inability of the privacy policy-based framework in achieving privacy within the organisations (Xiao & Pan, 2007).

The questionnaire established that a majority of the participants disagreed that the privacy policy was suited to their organisation's needs. There was a high level agreement with the unsuitability of the privacy policy together with an indication that they had not been consulted during the development of the privacy policy, even though their consultation had been done through effective methods such as interviews, polls, open days, surveys, discussions, and forums. In contrast, a vast majority of the developers agreed that the consultations of the users during policy development had actually taken place. These findings support the conclusion that privacy policy-based framework cannot provide the most suitable and the most relevant solutions to the privacy issues in an enterprise even when high levels of consultations are held with the users at the development phase of the privacy policy framework.

Most of the survey participants indicated that they need to be aware of the where and when their personal information is disclosed. These statistics reveal that the highest proportion of the users of the distributed systems is opposed to personal information disclosure without their knowledge. This aspect gives a different description of what the users consider as privacy in that they would want to have information about the disclosure of their personal information. This finding disputes such practices of companies' privacy policy that allow the disclosure of personal information without the knowledge of the users (Xiao & Pan, 2007).

Moreover, a majority of the respondents indicated that they needed to be informed when their personal information was disclosed. This finding aligns to the finding of numerous privacy violation incidents indicated in the survey. Perhaps, the high proportion of the respondents who indicated the need to be informed about the disclosure of their personal information is as a result of the high prevalence of privacy violation incidents despite the presence of the privacy policies (World Conference on Information Systems and Technologies & Rocha, 2013). In the same light, many of the respondents indicated the need for the ability to control the personal information disclosure and only a few did not indicate this need. This finding explains the impact of the high prevalence of privacy violation incidents as well as the unreliability of the privacy policy in ensuring the privacy of personal information for the users of the distributed systems. However, it is indicative of the inability to control the disclosure of one's personal information as a major barrier to the accomplishment of privacy within an organisation. Such categories of information as medical history and financial history are sometimes considered as secrets because of their potentials of creating an immense challenge to the owners when disclosed. Such

categories of information can make one respond defensively to the questionnaires without the consideration of the fewer risk classes of personal information and if the generalisation is made a setback is likely to present in the research.

The survey also established that the respondents needed a mechanism to offer them the full control of the private information disclosure. This finding is indicative of the need to transfer part of the privacy perspectives to the users by providing them means and technologies to control how, where, where, and with whom their private information is shared. This need is supported by the HIPAA requirements, which classify clinical information as high-risk information (Watfa, 2012). For the purposes of this research, the distributed systems design need to augment the privacy policy with the mechanisms to enable the user have full control of the disclosure of their private information.

Most of the participants showed agreement with the idea of logging of the history of personal activities. History logging provides information about the computer use at a later date. If personal information is logged, its analysis can provide an indirect disclosure of various aspects of private information through the logged transactions. In the end, a breach of the privacy requirements is highly possible. The agreement with the idea of history logging provides insights about the best way of providing privacy to the distributed systems' users, in that it is something they are comfortable with and understand the need for information to be logged for their own security as well as privacy. Moreover, half of the participants showed support to the ability to adjust involvement in privacy in order to reduce the effort needed to manage personal privacy. The ability of the systems' users to adjust their involvement can reduce the enterprises' workload of

ensuring privacy for all because some aspects of privacy would be decentralised to the users.

In overall, the research established a misalignment between the privacy policies, the expectations of the users as well as their perceptions of privacy. The distributed systems attract many privacy issues because of the large network of computers with different users. It comes so naturally that the developers of the privacy policies miss some aspects of the real privacy situation as experienced by the end users of the systems. In this research, the establishment of the deficiencies of the privacy policy framework, as well as the privacy expectations and perceptions of the users, has established a better meaning of the privacy. The results of the survey create a foundational argument in combining the distributed system architecture with the structuration theory approach to disambiguate privacy.

6.4 Implications of Findings - Is privacy perception measurable?

This research put forward that the PPF framework, which captures privacy perception as opposed to privacy content, overcomes the shortcomings associated with prior privacy-policy measurement through a privacy framework that is designed based on indication of privacy incidents using the proposed privacy button of this study. In this regard, the framework design follows the concept of emerging strategic demand of users.

All privacy perception measurement frameworks designed until now, including the privacy frameworks, rest upon mere counts of privacy incidents and the maintained

hypothesis that quantity and quality are positively related. It may be that privacy perception has defied direct measurement despite our best efforts to quantify it because privacy perception is inherently immeasurable.

6.5 Summary

To summarise, this chapter presented a discussion of the results and placed the results in the context of existing ideas found in the literature. Moreover, there was a discussion of the implications of the results in reference to the development of privacy policy frameworks based on the derived concerns and needs of users, such needs being derived through a disambiguation of the meaning of privacy. The discussion of the results was conducted within the structure of the proposed framework of this study. Specifically, the discussion focused on the results that provided information, ideas and implications related to existing privacy policy frameworks in the respective organisations, which form the technical / objective side of the framework and the results that were related to the privacy concerns and perception of privacy, and ultimately privacy expectations which form the lexical / subjective of the framework.

Chapter 7

Conclusion and Future Work

Objectives

- Provide a summary of the work carried out in this research.
- Overview of the findings, implications.
- Presents contributions of the study.
- Limitations of this research.
- Provide recommendations for future study.

7.1 Conclusion

This study was motivated by the fact that privacy policy written for distributed systems (DS) is written based on technical considerations and pays very little attention to the privacy needs of the users of distributed systems. This is especially a problem as such systems are increasingly complex which changes the level and type of privacy concerns of users. However, it was still important that during the development of privacy policy the technical parameters and constraints of DS should also be considered, therefore, there was a need to consider both these technical parameters and the privacy needs of users in the development of privacy policies. This was achieved through the development of a new privacy policy framework (PPF) that was essentially based on a hybridisation of the meaning of privacy derived from the technical considerations for DS and the meaning of privacy derived from users. A main function of the framework was to understand the meaning of privacy, specifically the meaning of privacy to users through understanding privacy perception and translating those perceptions into privacy expectations. Thus it was necessary to establish the semantic meaning of privacy and the perception of privacy through the disambiguation of privacy; this formed the part of the framework that was concerned with the subjective idea of privacy which formed one side of the lexical – technical meaning of privacy.

The research methodology had two main purposes in this study, firstly, to understand the current situation as regards current privacy policy and distributed systems towards a justification and development of the PPF, and secondly, to apply the developed framework through disambiguating privacy and an evaluation of the framework.

The research finds out that despite the fact that there is involvement and consideration of the distributed systems' users in the development of the privacy policy, the privacy situation remains challenged as indicated by a high number privacy violation incidents established by this research. The users' response to the questionnaire survey shows that enterprise privacy policy does not provide a complete definition of privacy because it misses addressing the preferences of the users that are biased towards helping them achieve the full control of their privacy. The users provided various subjective views about privacy which included the overall ability to control all aspects of their privacy. Therefore, it was shown that current approaches to privacy policy fail to achieve all the goals of privacy. The combination of the findings of deficient privacy policies created the need for a new approach to privacy through disambiguating its real meaning and not just the meaning that is assumed by those who are responsible for privacy policy in DS.

Importantly, the study did not place all of the emphasis on the need to base privacy policy based solely on the perceptions of privacy. Privacy policies are developed with technical considerations in mind, these considerations included technical requirements and constraints of distributed systems and the PPF allowed the consideration of these issues with privacy perceptions. In fact the PPF clearly considers the technical equally as it formed the other half of the lexical – technical construct. Therefore, the PPF demonstrated a way that both the lexical meanings and technical meaning could be considered at the same time creating a new way of considering privacy.

The application of the PPF was successfully demonstrated through the use of questionnaires and interviews to derive the perceptions of privacy and the technical considerations of DS. This was important in order to demonstrate the validity of the

framework. This demonstration can be used as a guide for future development of the framework or application of the framework itself. The interviews and questionnaires were also validated as tools suitable for deriving perceptions of privacy from expert's users and developers.

7.2 Contributions

The study has contributed to a new way of thinking about privacy in distributed systems. Because such systems are increasingly complex and personal information is widely shared and pervasive, then there is a need to reconsider privacy and develop beyond standard privacy policies. The PPF showed how individual concerns about privacy in distributed systems could be disambiguated and used in system development. Overall the rapid developments in technology, especially distributed technology, need to be matched with more relevant approaches to privacy provision, something the present study has achieved through creating a framework that considers up to date perceptions of privacy.

The inclusion of the perception of privacy as expectations into a privacy policy has not only had benefits in terms of simply including privacy perception in the development of such policies, but has also allowed a way the privacy policies themselves to become real-time and dynamic. This was achieved through the introduction of a button that allowed users to indicate the activities where they needed privacy when engaged in the distributed system. This allowed the idea of considering privacy perception to be extended to real time use of the system. This contribution has been particularly relevant to the developers of privacy policies because it allows them to understand privacy perception and expectations in real time as well as allowing users more participation in the development process.

Another contribution of the study is that it revealed the deficiencies of existing approaches to the development of privacy policy in distributed systems. Often the approaches were standard and did not fully consider the nature of distributed systems or the issue of private information in those systems, yet alone the needs and concerns of the users.

The development of a new PPF based on a hybridisation of the lexical and the technical derives numerous additional contributions as listed below:

- Progress privacy understanding in distributed system architectures, developers and users.
- To demonstrate how the lexical can be translated to the technical through deriving user expectation from user privacy perception.
- Improve understanding of distributed system design in linking perception to design in relation to privacy.

- To identify any significant issues related to the construct being developed in PPF framework and the likely impact on issues raised by individual users, developers and owners about the privacy policy that being developed.
- Contribute to the inclusion of privacy in development of distributed systems.
- Contribute to the development of privacy frameworks and a wider understanding of privacy towards system development generally.

7.3 Success Criteria

- Successful disambiguation of the meaning of privacy to users.
- Translation of user perception of privacy into user expectations.
- Development of PPF based on ideas found in structuration theory and hybridisation.

At the beginning of the study success criteria were established derived from the aims and objectives of the study. Overall, the main aim of the study was the development of a PPF which would be used as a new approach to develop privacy policy; this was successfully developed and demonstrated.

The first established criteria was the successful disambiguation of the meaning of privacy to users. The study successfully disambiguated the meaning of privacy from the users and developers of distributed systems using the questionnaires.

The second established success criteria was the translation of user perception of privacy into user expectations. As part of the proposed PPF the user perceptions were successfully translated into user expectations that can be used in the development of a new privacy policy.

The third success criteria was the development of a PPF based on ideas found in structuration theory and hybridisation. This was successfully achieved through the development of the PPF which was based on ideas about both the subjective, in this case the subjective perceptions of privacy, and the objective context in which this perception took place which was the technological considerations for privacy.

7.4 Limitations

Part of the research methodology involved the use of interviews and there are two associated limitations with this method. Firstly, the data had to be collected, transcribed and then interpreted and it is during this process that there can be bias from the researcher. Secondly, some of the respondents to the interviews may not want to be critical of their organisation's privacy policy and therefore, they may be some bias from them.

Although this research accomplished its aims, it faced several shortcomings. One of the limitations of this research is a lack of probability-driven sampling and the associated

lack of generalisability of the findings (Liamputtong & Ezzy, 2005). The interview was conducted on just ten senior managers despite a large number of firms using distributed systems across the globe. Besides, the interview questions of the senior managers were biased towards the U2U services without paying the due consideration of the numerous activities that can be accomplished through the distributed systems. The research is also highly qualitative and lacks much emphasis on numeracy hence it has a low scalability of the findings (GIVEN, 2008). Moreover, the research questionnaire had some open questions, and their assessment was based on the researchers' understanding of the responses and thus a certain level of subjectivity is present.

7.5 Future study

The future focus of the research in relation to this paper should focus on determining the methods/mechanisms of allowing the full control of one's personal control disclosure. The heavy bias of the respondents to the ability to control their personal information disclosure elicits the need to identify the effective mechanisms of allowing the full control of the personal information disclosure among the users of the distributed systems. However, the mechanisms identified should not discredit the enterprise' privacy policy, and thus the research should also focus on strengthening the privacy policy development by considering their deficient areas. This would be a development on the contribution of the button where the privacy needs can be provided in real time.

Moreover, advancement on the abovementioned idea would be to have a real time learning system using AI, whereby a privacy policy is not something that is developed in

one instance, but is something that is continually changing in response to users live indication about privacy concerns. Increased user engagement in privacy policy and provision by applying the PPF framework principles and methods such as flexibility, extendibility and permeability at the design stage, rather than a static privacy policy, may be more capable of meeting users changing privacy needs.

This thesis claims that privacy framework is an exemplar for integrating existing techniques and tools towards the design of usable PPF framework. In particular, privacy framework makes three significant contributions towards the stated research problem. First, a conceptual model for usable secure Infrastructure engineering is presented, upon which the privacy framework is founded; this meta-model informs changes to elicitation and specification techniques for improved interoperability in the design process. Second, several characteristics of methods needed to specify and disambiguate privacy are introduced; a set of criterion, constructors and guiding principle are used to illustrate how these characteristics can be embodied. Third, how the results of applying PPF framework can be used to improve the design of existing User-Centred Design techniques for privacy policy design is described. This thesis brings forth a number of important questions related to privacy perception. What defines privacy perception? Is privacy perception measurable? Is the maintained hypothesis that privacy perception measurements are positively related and descriptive? These are critically important questions about which very little is known. They are worthy of careful evaluation, and addressing these questions may represent a necessary next step in the advancement of privacy research. I suspect that while some of these questions may be answerable in a general setting (e.g., what defines privacy perception?), others and the development of universal privacy perception

frameworks for assessing privacy perception must be addressed in the context of a specific research question. This study also draws out a number of important questions related to privacy breaches. What information aids developers in their estimation of number of privacy perception incidents? How do managers use this information in developing their decisions to deal with conflict perception semantics? Do developers use number of privacy perception incidents to assess divisible, non-divisible privacy perception and uncertainty? How do developers' perceptions of privacy impact the number of privacy perception incidents? These too are difficult but critically important questions to consider. But, these questions extend well beyond the boundaries of privacy research, such as, in the field of behavioural computation, and or, neural computation.

The thesis is validated by applying the privacy framework is used to specify privacy requirements, such as, understand-ability, relevance, reliability and compare-ability for a privacy provision model. The privacy framework is used to specify infrastructure requirements for a meta-data repository. Finally, the privacy framework is used to analyse a proposed privacy attributes mainly privacy perception and number of incidents, and also, the privacy framework is applied within the context of an action research intervention, where findings and lessons from one case study are fed into the action plan of the next.

Bibliography

Acquisti, A, Brandimarte, L, & Loewenstein, G 2015, 'Privacy and human behaviour in the age of information', *Science*, 347, 6221, pp. 509-514.

Alhalafi, D. (2015). A New Methodology to Disambiguate Privacy. Acta Physica Polonica A. 28 (2B), 319 - 323.

Almeida, D. Poell, D (2012). New Privacy Framework Poses Challenges for Digital Stakeholders; *Consumer & Personal Rights Litigation*, 15, 1, pp. 2-5.

Andrews, Gregory R. (2000). Foundations of Multithreaded, Parallel, and Distributed Programming, Addison–Wesley, ISBN 0-201-35752-6. p32.

Anthonysamy, P. G. P., & Rashid, A. (2013) Social Networking Privacy: *understanding the disconnection from policy to controls*.

Antón, A, Bertino, E, Ninghui, L, & Ting, Y 2007, 'A Roadmap for Comprehensive Online Privacy Policy Management', *Communications of the ACM*, 50, 7, pp. 109-116.

Anton, A. Breaux, T. Gritzalis, S. Mylopoulos, J. (2011). Digital privacy: theory, policies and technologies. Requirements Engineering. 16, 1 - 2.

Anton, A.I., Earp, J.B. & Young, J.D. 2010, "How internet users' privacy concerns have evolved since 2002", IEEE Security & Privacy, vol. 8, no. 1, pp. 21-27.

Aved, A, & Hua, K (2012). 'A general framework for managing and processing live video data with privacy protection', *Multimedia Systems*, 18, 2, pp. 123-143.

Balouziyeh, J, & Hussein, A (2012). 'The Legal Framework for Privacy and Data Protection in Saudi Arabia, *International Law News, 41, 4, p.19.*

Beekhuyzen, Jenine, Nielsen, Sue, & Von Hellens, Liisa. (2003). *Challenging Dualisms in Female Perceptions of IT Work*. Australasian Journal of Information Systems. 10 (2).

Bellamy, C, & Raab, C 2005, 'Multi-agency working in British social policy: Risk, information sharing and privacy', *Information Polity: The International Journal of Government & Democracy in the Information Age*, 10, 1/2, pp. 51-63. d

Calo, MR (2011). 'The Boundaries of Privacy Harm', *Indiana Law Journal*, 86, 3, pp. 1131-1162.

Cambridge Dictionaries Online. (2014). Available: http://dictionary.cambridge.org/dictionary/english/privacy. Last accessed 1st December, 2014.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*. 11, 431-448.

Campisi, P. (2013). *Security and privacy in biometrics*. London, Springer:http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&A N=604387.[Accessed:19/03/14].

Cao, Z, Li, K, Li, X, Mcdaniel, P, Poovendran, R, Wang, G, & Xiang, Y (2014), 'Guest Editors' Introduction: Special Issue on Trust, Security, and Privacy in Parallel and Distributed Systems', *IEEE Transactions on Parallel & Distributed Systems*, 25, 2, pp. 279-282.

Carroll, J. (2006). *Privacy*. Detroit, Greenhaven Press.

cdt.org (2014) Comprehensive Privacy and Security: Critical for Health Information Technology.

Chander, A., Gelman, L., & Radin, M. J. (2008). Securing privacy in the Internet age. Stanford, Calif, Stanford Law Books.

Council Of Europe. (2002). *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows.* Strasbourg, Council of Europe.

Cranor, L.F., M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle, (2000) *The Platform for Privacy Preferences* 1.0 (P3P1.0) Specification, W3C Working Draft, http://www.w3.org/TR/P3P/. [Accessed: 28/07/2015].

Daniel J. S. (2004) the Digital Person: *Technology and Privacy in the Information Age*, (Publisher New York University Press.

Dasgupta, A, Chen, M, & Kosara, R 2013, 'Measuring Privacy and Utility in Privacy-Preserving Visualization', *Computer Graphics Forum*, 32, 8, pp. 35-47.

Data Collection Policy Prompts Privacy Concerns' 2015, *Information Management Journal*, 49, 5, p. 6.

Data Protection Act 1998. (c.29).section 2. London: HMSO

Dawes, S. (2008) Governance in the information age: a research framework for an uncertain future‘, Proceedings of the 2008 international conference on Digital government research. Montreal, Canada.

Deng, M, Wuyts, K, Scandariato, R, Preneel, B, & Joosen, W 2011, 'A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements', *Requirements Engineering*, 16, 1, pp. 3-32.

Donovan, C (2004). 'Implementation of the e-Privacy Directive in the UK – understanding the new rules', *Computer Law & Security Review*, 20, 2, p. 127.

Doris, M.J (2010). 'Daniel J Solove, UNDERSTANDING PRIVACY’ Cambridge, MA: Harvard University Press.

Fisher, D (2003). 'IBM taking privacy to next level. (Cover story)', *Eweek*, 20, 48, pp. 1-18.

Flavián, C. Guinalíu, M (2006),"Consumer trust, perceived security and privacy policy", Industrial Management & Data Systems, Vol. 106 Iss 5 pp. 601 - 620

Gandy, OH 2003, 'Public Opinion Surveys and the Formation of Privacy Policy', *Journal of Social Issues*, 59, 2, pp. 283-299.

Ghinita, G, Karras, P, Kalnis, P, & Mamoulis, N (2009), 'A Framework for Efficient Data Anonymization under Privacy and Accuracy Constraints', *ACM Transactions on Database Systems*, 34, 2, pp. 9-4.

Gillham, B (2000). The Research Interview. London: Continuum.

Given, L. M. (2008). *The Sage encyclopedia of qualitative research methods*. Los Angeles, Calif, Sage Publications.

Gong, S., Cristani, M., Yan, S., Loy, C.C. (2014), *Person Re-Identification*, Springer.

Google and UK Call a Truce on Privacy Policy' 2015, *Information Management Journal*, 49, 2, p. 11.

Graber, M, D'Alessandro, D, & Johnson-West, J 2002, 'Reading level of privacy policies on Internet health Web sites', *Journal Of Family Practice*, 51, 7, pp. 642-645.

Haftor, D. M., Mirijamdotter, A., & Bradley, G. (2011). *Information and communication technologies, society and human beings theory and framework.* Hershey, Pennsylvania.

Halboob, W, Mahmod, R, Udzir, N, & Abdullah, M 2015, 'Privacy policies for computer forensics', *Computer Fraud & Security*, 2015, 8, pp. 9-13.

Hans, GS 2012, 'Privacy Policies, Terms Of Service, And Ft. Enforcement: Broadening Unfairness Regulation For A New Era', *Michigan Telecommunications & Technology Law Review*, 19, 1, pp. 163-20.

Hawk, S, Raaijmakers, Q, Hale Iii, W, & Meeus, W (2008). 'Adolescents' Perceptions of Privacy Invasion in Reaction to Parental Solicitation and Control', *Journal of early Adolescence*, 28, 4, pp. 583-608.

Hier, S, & Walby, K 2014, 'Policy Mutations, Compliance Myths, and Redeployable Special Event Public Camera Surveillance in Canada', *Sociology*, 48, 1, pp. 150-166.

http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=518635. [Accessed: 15/11/2014].

http://www.guardian.co.uk/technology/2013/may/16/internet- of-things-privacygoogle. [Accessed 20/09/2015.

Huang, X, Xiang, Y, Chonka, A, Zhou, J, & Deng, R (2011). 'A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems', *IEEE Transactions On Parallel & Distributed Systems*, 22, 8, pp. 1390-139.

Ifip World Computer Congress, & Deswarte, Y. (2004). *Information security management, education and privacy IFIP 18th World Computer Congress: TC11 19th International Information Security Workshops 22-27 August 2004, Toulouse, France* Boston, Mass, Kluwer Academic Publishers.

International Conference on Information Systems Design And Intelligence Applications, & Mandal, J. K. (2015). *Information systems design and intelligent applications: proceedings of Second International Conference India 2015. Volume 2.*

Jia, W., & Zhou, W. (2005). *Distributed network systems from concepts to implementations*. New York, Springer. http://site.ebrary.com/id/10228907.

Jones, M (2003) Structuration Theory. In Currie, W. Galliers, R eds. 2003 Rethinking Management Information Systems: An Interdisciplinary Perspective. Oxford University Press. Oxford pp. 103 – 105.

Jones, M. Karsten, H. (2003). Review: Structuration Theory And Information Systems Research. Judge Institute of Management, University of Cambridge.

Kadloor, S, Gong, X, Kiyavash, N, & Venkitasubramaniam, P 2012, 'Designing Router Scheduling Policies: A Privacy Perspective', *IEEE Transactions on Signal Processing*, 60, 4, pp. 2001-2012.

Karat, J, Karat, C, Bertino, E, Li, N, Ni, Q, Brodie, C, Lobo, J, Calo, S, Cranor, L, Kumaraguru, P, & Reeder, R (2009), 'Policy framework for security and privacy management', *IBM Journal Of Research & Development*, 53, 2, PP. 4: 1-4:14.

Keizer, G. (2012). *Privacy*. New York, Picador.

King, N. Horrocks, C (2010). Interviews in Qualitative Research. London: SAGE Publications.

Klosek, J. (2000). *Data privacy in the information age*. Westport, Conn, Quorum Books.

Kuchinke, W, Ohmann, C, Verheij, R, Van Veen, E, Arvanitis, T, Taweel, A, & Delaney, B (2014), A standardised graphic method for describing data privacy frameworks in primary care research using a flexible zone model', *International Journal of Medical Informatics*, 83, 12, pp. 941-957.

Kvale, S (2007). Doing Interviews. London: SAGE Publications.

Laudon, K. C., & Traver, C. G. (2013). *E-commerce: business, technology, society*.

Lee, P. (2013) *A Brave New World Demands Brave New Thinking* (IAPP Privacy Perspectives, May 28, 2013).

Lee, T. (2012), *the Media, Cultural Control and Government in Singapore* (Routledge Media, Culture and Social Change in Asia), Publisher: Routledge.

Liamputtong, P., & Ezzy, D. (2005). *Qualitative research methods*. South Melbourne, Vic, Oxford University Press.

Manon, A, Jacques, N, Mathieu, A, & Anne, V (2007). 'The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust', *Online Information Review*, 31, 5, pp. 661-681.

Mekovec, R. & Vrcek, N. 2011, "Factors that influence Internet users' privacy perception", , pp. 227.

Merriam Webster (2014). Full Definition of privacy. Available: http://www.merriam-webster.com/dictionary/privacy. Last accessed 1st December, 2014.

Micheti, A, Burkell, J, & Steeves, V 2010, 'Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand', *Bulletin of Science, Technology & Society*, 30, 2, pp. 130-143.

Miyazaki, A, & Fernandez, A (2001). 'Consumer Perceptions of Privacy and Security Risks for Online Shopping', *Journal of Consumer Affairs*, 35, 1, p. 27.

Miyazaki, A, & Krishnamurthy, S 2002, 'Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions', *Journal of Consumer Affairs*, 36, 1, p. 28.

Molloy, Padraig, Golden, William, & Kirwan, Orla. (2008). *Energy Management Information Systems: An Exploratory Study of Implementations Using Adaptive Structuration Theory*. *http://hdl.handle.net/10379/71*.

Mont, M, & Thyne, R 2008, 'Privacy policy enforcement in enterprises with identity management solutions', *Journal of Computer Security*, 16, 2, pp. 133-163.

Mooradian, N 2014, 'Closing the Gap between Policy and ECM Implementation Using Privacy by Design', *Information Management Journal*, 48, 5, pp. 20-26.

Nabeel, M, Shang, N, & Bertino, E 2013, 'Privacy Preserving Policy-Based Content Sharing in Public Clouds', *IEEE Transactions On Knowledge & Data Engineering*, 25, 11, pp. 2602-2614.

Nadas, A, Levendovszky, T, Jackson, E, Madari, I, & Sztipanovits, J 2014, 'A model-integrated authoring environment for privacy policies', *Science Of Computer Programming*, 89, Part B, pp. 105-125.

Nan, Z, & Wei, Z (2008), 'Privacy Protection against Malicious Adversaries in Distributed Information Sharing Systems', *IEEE Transactions On Knowledge & Data Engineering*, 20, 8, pp. 1028-1033.

NEWMAN, J 2015, 'AVG's new privacy policy is uncomfortably honest about tracking users', *PC World*, pp. 63-64.

Paine, C, Reips, U, Stieger, S, Joinson, A, & Buchanan, T (2007). 'Internet users' perceptions of 'privacy concerns' and 'privacy actions'', *International Journal of Human-Computer Studies*, 65, 6, pp. 526-536.

Papanikolaou, N, Creese, S, & Goldsmith, M 2012, 'Refinement checking for privacy policies', *Science of Computer Programming*, 77, 10/11, pp. 1198-1209.

Park, N, & Kim, M 2014, 'Implementation of load management application system using smart grid privacy policy in energy management service environment', *Cluster Computing*, 17, 3, pp. 653-664.

Pollach, I. (2008). Privacy Statements as a Means of Uncertainty Reduction in WWW Interactions. In: Clarke, S End User Computing Challenges and Technologies: Emerging Tools and Applications. New York: IGI Publishing. 188 - 208.

Pollach, I 2007, 'WHAT'S WRONG WITH ONLINE PRIVACY POLICIES?' *Communications of the ACM*, 50, 9, pp. 103-108.

Proctor, R, Ali, M, & Vu, K 2008, 'Examining Usability of Web Privacy Policies', *International Journal of Human-Computer Interaction*, 24, 3, pp. 307-328.

Putnam, L., & Mumby, D. K. (2014). *The Sage handbook of organizational communication: advances in theory, research, and methods.*

Raghunathan, B. (2013) *The Complete Book of Data Anonymization: From Planning to Implementation*, Auerbach Publications.

Reenleaf, G, Chung, P, & Mowbray, A 2015, 'Supporting and influencing data privacy practice: The free access International Privacy Law Library', *Computer Law & Security Review*, 31, 2, pp. 221-233.

Rubel, A, & Biava, R (2014), 'A framework for analysing and comparing privacy states', *Journal of The Association For Information Science & Technology*, 65, 12, pp. 2422-2431.

Sandhu, R., S. Osborn and Q. Munawer. (2000). 'Configuring role-based access control to enforce mandatory and discretionary access control policies'. *ACM Transactions on Information and SystemSecurity*, 3(2): pp. 85-106.

Schaffer, K 2013, 'Passwords, Privacy, and Policies: Can They Do Business Together?', *Computer*, 46, 12, pp. 76-79.

Schneier, B. (2013) 'Will Giving the Internet Eyes and Ears Mean the End of Privacy? (The Guardian May, 16, 2013

Sevignani, S 2013, 'The commodification of privacy on the Internet', *Science & Public Policy (SPP)*, 40, 6, pp. 733-739.

Shuler, J 2004, 'INFORMATION POLICY Privacy and Academic Libraries: Widening the Frame of Discussion', *Journal of Academic Librarianship*, 30, 2, pp. 157-159.

Simons, C, & Wirtz, G (2007). 'Modelling context in mobile distributed systems with the UML', *Journal of Visual Languages & Computing*, 18, 4, pp. 420-439.

Appendix A

1. Interview schedule

1. Does your privacy policy offer the best service to its users?

2. Could you tell me about any privacy issues in the DS?

3. How does the DS support user services?

4. Could you tell me in your opinion about the effectiveness of the privacy policy?

5. How is the privacy policy developed and by whom?

6. Do you consider accessibility of the privacy policy?

7. Does your privacy policy consider those with disability and their access?

2. Questionnaire

This questionnaire is part of a study to understand the issue of privacy in distributed systems. The questionnaire is divided into two main sections, the first section aims to discover the current situation in your organisation as regards privacy policy, and the second section aims to understand your own perception of privacy in relation to the information systems you use. Anonymity is assured and if there are any questions please contact the researcher at d_alhalafi@yahoo.co.uk .

Section A. Current Privacy Policy

1. On which platform does your distributed system sit?

_____

_____

_____

_____

2. Are you aware of the function of the enterprise privacy policy?

_____

_____

_____

_____

3. What is your opinion about the enterprise privacy policy?

_____

_____

_____

4. Please list any events where the privacy policy has protected you

_____

_____

_____

5. In your opinion, what are the reasons behind the lack of enthusiasm towards the enterprise privacy policy?

_____

_____

_____

6. Please describe any incidents where your privacy was violated at work

_____

_____

_____

7. The privacy policy is effective in terms of making you feel secure

Strongly agree ☐ Agree ☐ Undecided ☐ Disagree ☐
Strongly disagree ☐

8. The privacy policy suits your / organisation's needs

Strongly agree ☐ Agree ☐ Undecided ☐ Disagree ☐
Strongly disagree ☐

9. I am consulted in the development of the privacy policy (users)

Strongly agree ☐ Agree ☐ Undecided ☐ Disagree ☐
Strongly disagree ☐

10. How are you consulted about your privacy needs

_____

_____

_____

11. How is your privacy policy developed? (developers)

_____

_____

_____

12. Users are consulted about their needs in the development of the framework? (developers)

Strongly agree ☐ Agree ☐ Undecided ☐ Disagree ☐

Strongly disagree ☐

Section B. Privacy Perception

I should be aware of where and when my information is disclosed

Strongly agree ☐ Agree ☐ Undecided ☐ Disagree ☐

Strongly disagree ☐

I should be informed of when my information is disclosed

Strongly agree ☐ Agree ☐ Undecided ☐ Disagree ☐

Strongly disagree ☐

I should be able to control where and when my private information is disclosed

Strongly agree ☐ Agree ☐ Undecided ☐ Disagree ☐

Strongly disagree ☐

I need a mechanism to have full control over what I think should be private

Strongly agree ☐ Agree ☐ Undecided ☐ Disagree ☐

Strongly disagree ☐

I am comfortable with the history of my activities being logged

Strongly agree ☐ Agree ☐ Undecided ☐ Disagree ☐

Strongly disagree ☐

I should be able to adjust involvement in privacy in order to reduce the effort needed to manage my privacy

Strongly agree ☐ Agree ☐ Undecided ☐ Disagree ☐

Strongly disagree ☐